International Journal of Safety and Security Engineering
Vol. 16, No. 5, May, 2026, pp. 1091-1102
Journal homepage: http://iieta.org/journals/ijsse

A Multi-Layer Visual Cryptography Framework with Adaptive Key Optimization and Kronecker Product-Based Diffusion

Sachin M. Kolekar*, Pushpalata Ganesh Aher

School of Computer Science & Engineering, Sandip University, Nashik 422213, India

Corresponding Author Email: sachinalways24@gmail.com

https://doi.org/10.18280/ijsse.160514

Received: 27 February 2026
Revised: 7 April 2026
Accepted: 25 May 2026
Available online: 31 May 2026

Keywords:
visual cryptography, Improved Gold Rush Optimization, Kronecker product diffusion, elliptic curve cryptography, image security, metaheuristic optimization, secret image sharing

ABSTRACT

Visual cryptography (VC) enables secure sharing of images by dividing a secret image into multiple shares; however, existing VC methods often suffer from pixel expansion, weak key selection, and limited robustness. To address these challenges, this work introduces an Improved Gold Rush Optimization (IGRO) algorithm for optimal key selection in a Kronecker product–based VC framework. The proposed system integrates multiple encryption layers, including Baker chaotic permutation, elliptic curve cryptography (ECC), one-time pad (OTP) masking, and Kronecker product–based diffusion, to enhance security and visual quality. IGRO improves upon the conventional Gold Rush Optimization by incorporating adaptive diversification and hybrid search strategies, enabling faster convergence and avoidance of local optima. Experimental results on standard test images demonstrate that the IGRO-based scheme achieves high reconstruction quality, with peak signal-to-noise ratio (PSNR) values up to ~82 dB and structural similarity index measure (SSIM) between 0.81 and 0.83, while significantly reducing error metrics such as bit error rate (BER), mean absolute error (MAE), and mean squared error (MSE) by 2–3 times compared to state-of-the-art optimizers, including Harris Hawks Optimization (HHO), Moth-Flame Optimization (MFO), Naked Mole-Rat Algorithm (NMRA), Slime Mould Algorithm (SMA), and Gold Rush Optimization (GRO). Security analysis further confirms strong resistance against statistical, noise, filtering, and geometric attacks, ensuring high fidelity of the reconstructed images. Overall, IGRO provides an efficient and robust optimization strategy that significantly enhances both cryptographic strength and visual performance in multi-layer VC systems.

1. INTRODUCTION

Visual cryptography (VC) is a paradigm of image encryption where a secret image is divided into shares in a way that only a person with enough shares can be able to reconstruct the secret which is visual in nature [1]. Naor and Shamir [2] were the first to use it in 1994 in the area of voting, finance and privacy protection. The traditional VC schemes have problems such as pixel expansion, high cost of computation and poor quality of image when decrypted [3]. These problems have been overcome in recent works by applying VC in combination with optimization and cryptography. As an example, Ibrahim et al [4] utilizes Harris Hawks Optimization (HHO) to select color sub-pixels in a VC scheme in an optimal manner, yielding non-expanded shares with a better reconstruction quality. This increased the peak signal-to-noise ratio (PSNR) and speed of encryption compared to simpler VC techniques, which are aided by metaheuristics. However, to withstand different attacks, more effective key generation and enhanced security are still required.

For instance, Kanwal et al. [5] combined ECC key generation with 3D Chebyshev chaotic maps to create a hybrid image cipher that showed high entropy and strong resistance to statistical attacks (NPCR ≈ 99.6%, UACI ≈ 33.4%). one-time pad (OTP) encryption, which is also based on perfect key secrecy, could be computationally unbreakable by XORing the pixels in an image with keys which are really random [6]. More modern color image encryptions have used one-time chaotic keys (e.g. rotor-machine concept) to permute and XOR image data, which has proven to be sufficiently confusing [7]. These advances highlight that the perfect visual cryptosystem must employ a multi-layered strategy: secret sharing of VC, chaotic permutation to diffusion, OTP/XOR to confusion and secure key exchange (elliptic curve cryptography (ECC) - with an optimization algorithm to select the best keys.

In the last couple of years, metaheuristic optimization algorithms have become widespread, and have been used to enhance cryptographic systems [8]. Famous ones are HHO [6], Moth-Flame Optimization (MFO) [9], Naked Mole-Rat Algorithm (NMRA) [10], Path Finder Algorithm (PFA) [11], Poor and Rich Optimization (PRO) [12], Slime Mould Algorithm (SMA) [13], etc. HHO is a swarm intelligence method inspired by hawks' cooperative hunting; it has outperformed classical optimizers like PSO and GA on many benchmarks [14] and has seen use in VC and steganography for selecting optimal encoding parameters. MFO is a nature-inspired algorithm modeling moth navigation, known for good

exploration-exploitation balance. NMRA imitates the mating behavior of mole-rats and has shown competitive performance, though it may suffer premature convergence. New human-based algorithms have also emerged: PRO, for instance, models socio-economic behavior of rich and poor classes to guide search, and demonstrated superior exploration on engineering design problems [15]. Many of these algorithms have been employed in image encryption or VC contexts – e.g. a binary dragonfly algorithm to optimize color levels in VC shares [16], or a genetic algorithm (GA) combined with chaos and ECC to optimize encryption keys [17]. The Gold Rush Optimization (GRO) algorithm is a relatively recent human-inspired optimizer introduced by Zolfi Kamran et al, based on the decision-making of gold prospectors in a gold rush scenario [18]. GRO models a group of individuals searching for gold, where human reasoning guides exploration and exploitation, rather than animal behavior or physics laws. This approach showed successful results on structural optimization tasks. Recognizing the potential of GRO's unique search strategy, we propose an improved variant for cryptographic key optimization.

Despite these advancements, existing VC and image encryption methods still face several challenges, including suboptimal key selection, limited balance between security and reconstruction quality, and premature convergence in optimization-based approaches. Many current techniques rely on conventional metaheuristic algorithms that may not effectively explore the large cryptographic search space generated by chaotic and ECC-based systems. Furthermore, the integration of optimization strategies with multi-layer VC frameworks remains insufficiently explored. To address these limitations, this work introduces an Improved Gold Rush Optimization (IGRO) algorithm for efficient cryptographic key optimization within a hybrid VC architecture.

This paper presents a novel optimization algorithm, termed as IGRO, to enhance a Kronecker product-based VC scheme. Our aim is to efficiently generate optimal encryption keys that improve both the security and quality of the VC encryption-decryption process. We integrate IGRO into a multi-stage image encryption architecture comprising ECC, OTP keying, Kronecker product expansion, and Baker's chaotic map. By doing so, the proposed scheme leverages IGRO to navigate the large key space introduced by chaotic and ECC parameters, yielding near-optimal keys for robust encryption.

The contributions of this work are summarized as follows:

- To design a hybrid VC system with multiple encryption layers, all orchestrated by IGRO for key optimization.
- To extensively compare IGRO-VC scheme with the current techniques by the means of standard image quality measures, error measures and security tests such as statistical tests and resistance to filtering, noise, and rotation attacks.
- Convergence analysis and statistical significance testing are presented by us to prove the efficiency and reliability of IGRO.

The structure of the paper is the following. Section 1 presents the introduction to the work, explaining problems of VC schemes, and contributions of the work. Section 2 provides the analysis of the related literature, discussing VC schemes, cryptographic improvements ECC and pointing out gaps in the research. Section 3 explains the methodology, including the system architecture and embedding and extraction processes, as well as a multi-stage encryption pipeline. Also, an algorithm is developed with the IGRO algorithm and explains how it is superior to generate optimal keys is discussed. In section 4, the experiment setup including environment, dataset and parameter are explained and contains detail result analysis and discussion. Section 5 conclude the work with important results and provides the future scope, and references are set at end of paper.

2. LITERATURE REVIEW

This section presents a literature review of metaheuristic optimization algorithms, VC methods, and advanced image encryption algorithms, highlighting their methodologies, strengths, and limitations of research works.

2.1 Metaheuristic optimization algorithms

Metaheuristic optimization algorithms have gained significant attention for solving complex nonlinear and high-dimensional optimization problems due to their ability to effectively balance exploration and exploitation. Various nature-inspired and human-behavior-inspired optimization techniques have been proposed in the literature to improve convergence speed, solution quality, and robustness across diverse application domains.

Several nature-inspired and human-based metaheuristic algorithms have been developed to improve exploration, exploitation, convergence accuracy, and robustness in complex optimization problems. The NMRA was developed based on the eusocial behavior of mole-rat colonies, and its improved version further refines the exploration and exploitation stages to enhance node localization in wireless sensor networks (WSNs), achieving better 2D and 3D localization performance than conventional swarm optimizers [10]. The Pathfinder Algorithm (PFA) is another nature-inspired method based on leadership hierarchy and collective movement, in which a leader guides followers toward promising solutions; it has shown competitive convergence speed and solution accuracy in benchmark and engineering optimization problems [11]. Human-based multi-population strategies have also been explored, such as PRO, which models wealth-distribution behavior by dividing individuals into poor and rich populations [12].

In addition, the SMA, inspired by the oscillatory foraging behavior of slime mould organisms, uses dynamic weights to balance exploration and exploitation and has demonstrated strong performance in nonlinear and multimodal optimization problems [13]. HHO, which simulates the cooperative hunting and surprise-pounce strategies of Harris hawks, has been widely applied in feature selection, image segmentation, and engineering optimization [14]. Improved PRO further enhances convergence accuracy and robustness, showing superior performance on benchmark functions and constrained optimization problems [15]. For color visual cryptography schemes, the Binary Dragonfly Algorithm has been applied to optimize share generation and improve reconstruction quality and security strength [16]. The GRO, inspired by gold prospecting behavior, employs adaptive exploration mechanisms to avoid premature convergence and has shown competitive performance compared with established swarm-based algorithms [18].

2.2 Encryption and visual cryptography techniques

Several cryptographic and VC methods have also been developed to improve security, reconstruction quality, and computational efficiency. A chaotic image encryption protocol integrating ECC and GA was proposed to enhance randomness, resistance to statistical attacks, and overall encryption strength [17]. Cryptographic algorithms based on discrete mathematical concepts have also been applied to improve information security in WSNs, enhancing encryption efficiency and secure key management while maintaining robustness against potential security threats [19].

In the field of VC, an efficient framework for secure image sharing on social networks was developed to maximize reconstruction clarity while minimizing computational cost [20]. A lightweight XOR-based VC scheme with random shares was further introduced to reduce computational complexity while maintaining a high level of security, making it suitable for resource-constrained environments [21]. In addition, a multi-carrier VC technique based on XOR and OR operations was proposed to improve reconstruction accuracy and strengthen resistance to brute-force and differential attacks [22].

2.3 Advanced visual cryptography schemes

A region-incrementing VC scheme was proposed to support both OR and XOR decryption [23]. Unlike classical VC techniques based only on OR stacking, this scheme increases selected regions in the encrypted image to improve contrast and reconstruction quality. The incorporation of XOR operations further enhances flexibility and security. Experimental results show that the scheme achieves better visual quality with lower pixel expansion, making it suitable for secure image-sharing applications that require computational efficiency and flexible decryption.

An image encryption algorithm based on an Logistic-Bernoulli (LB) compound chaotic map was introduced to improve encryption security [24]. The method adopts a plaintext-based key generation scheme, in which encryption keys vary dynamically with input images. This design strengthens resistance against known-plaintext and chosen-plaintext attacks. Its randomness and key sensitivity were also statistically validated.

Recent advances in chaotic image encryption have also been reviewed, with emphasis on the role of chaotic maps in achieving high randomness, strong diffusion, and improved image security [25]. Existing challenges and future research directions for developing more robust and efficient image encryption systems were also discussed.

A secure medical image cryptography method based on DNA cryptography combined with ECC was proposed to improve data confidentiality while maintaining computational efficiency [26]. By encoding pixel values into DNA sequences and using ECC-based key exchange mechanisms, the scheme shows resistance to both differential and statistical attacks. It is therefore suitable for secure telemedicine and cloud-based medical data communication.

An encryption system combining the Kronecker product of finite fields with DNA operations was also developed to improve diffusion and confusion characteristics while preserving algebraic security [27]. Experimental results indicate high entropy and a large key space, showing strong resistance to brute-force and differential attacks.

3. METHODOLOGY

3.1 System architecture

The proposed scheme is based on a common embed-extract VC scheme with several encryption transformations added. The overall architecture in Figure 1 is separated into two major stages, namely: (1) Embedding (Encryption) stage and (2) Extraction (Decryption) stage. During the embedding, the secret images are initially divided and coded into a sequence of common images by the use of a probabilistic (2, 2) secret sharing method. We use this method of the initial share generation: a secret image is broken into several fragments and each fragment is stored in a random binary grid so that when the shares are shared, they can offer no information. This produces three encrypted shares subjectively random. These shares are then progressively encrypted through a series of stages:

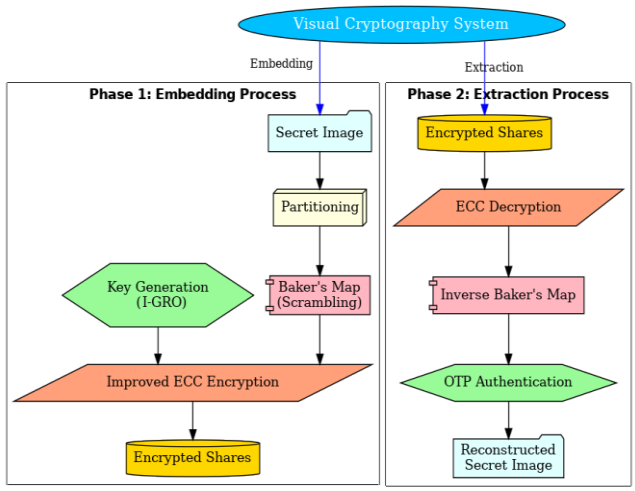


Figure 1. Proposed system architecture

3.1.1 Stage 1: Chaotic permutation with Baker's map

Each share undergoes pixel shuffling using the Baker's map, a 2D chaotic map often used for image permutation. The Baker's map treats the image as a unit square and "mixes" the pixels by stretching and folding operations akin to shuffling a deck of cards. Here it serves to diffuse the pixel positions thoroughly [24, 25]. By the end of this stage, each share's pixels are scrambled, removing any residual patterns. We denote the output as Baker-encrypted shares. This operation, being keyless, primarily adds confusion; however, the chaotic behavior ensures that without knowing the exact map iterations, reversing is difficult. The Baker's Map chaotic permutation used for scrambling the encrypted share image of size $N \times N$ is mathematically defined as:

$$B(x,y) = \begin{cases} \left(2x, \frac{y}{2}\right), & 0 \le x < \frac{N}{2} \\ \left(2x - N + 1, \frac{y+N}{2}\right), & \frac{N}{2} \le x < N \end{cases}$$

where,

- (x, y) represents the spatial coordinates of a pixel in the image,
- N denotes the image dimension,
- $B(x, y)$represents the transformed pixel position after chaotic permutation.

3.1.2 Stage 2: Improved elliptic curve cryptography (IECC) with one-time pad

Next, we enhance each share's encryption using an elliptic curve cryptosystem combined with OTP keys. In this encryption, each Baker-scrambled share is encrypted by a symmetric key derived from ECC and OTP. Specifically, we use an elliptic curve to generate a pair of public/private keys and a shared secret point; from that we derive a random pad which serves as a one-time XOR mask for the share pixels. Using a fresh OTP for each encryption ensures semantic security – even if the same image were encrypted again, a different random key would produce a completely different cipher image. The term "Improved ECC" here signifies that instead of directly applying ECC to the entire image, we use ECC only to securely generate and share the OTP key, combining the speed of symmetric XOR with the security of ECC key exchange. This hybrid approach leverages ECC's strong security and OTP's perfect secrecy. Similar ECC-based hybrid ciphers have shown high security and efficiency in medical image protection. After this stage, we obtain three IECC-encrypted shares. The improved ECC encryption process applied to the share image S using the one-time password (OTP) key K_{otp} is mathematically represented as:

$$C = S + K_{otp} + P$$

where,

- C denotes the encrypted cipher share,
- S represents the input share image,
- K_{otp} is the one-time encryption key,
- P is a selected point on the elliptic curve.

The OTP key generated using the MHOTP mechanism at time instance t is mathematically expressed as:

$$K_{otp}(t) = \text{HMAC} - \text{SHA256}(K_{secret}, t) \bmod 2^d$$

where,

- $K_{otp}(t)$ denotes the generated one-time encryption key at time instance t,
- K_{secret} represents the shared secret key between communicating entities,
- t denotes the timestamp or synchronization counter,
- $\text{HMAC} - \text{SHA256}(\cdot)$ is the hash-based message authentication code using the SHA-256 hashing algorithm,
- d represents the required key length in bits.

3.1.3 Stage 3: Kronecker product diffusion

The IECC-encrypted shares are then diffused using a Kronecker product-based operation. The Kronecker product (denoted $\otimes$) of two matrices is a larger matrix that intermixes their contents; here we use it to expand and entangle share data with a binary key matrix. In practice, we generate a pseudorandom binary matrix K of size $m \times n$ (derived from an IGRO-optimized seed), and compute $C = S \otimes K \; XOR \; K$, where S is an IECC-encrypted share (in binary form). This operation is essentially a scaling up of the share and distributing every bit of S into a submatrix with K weighting and introducing another level of confusion and sensitivity of the cipher to the key [27]. Kronecker-based transformations were also mentioned in a similar study by Mfungo et al. [28], who paired a Kronecker XOR product with a Hill cipher to amplify the diffusion and size of images, which produced a strong encryption against statistical and differential attacks. In our scheme, after applying the Kronecker product diffusion, we get three diffused share images. These shares are significantly randomized and enlarged, with minimal correlation to the original secret. The Kronecker product-based encryption between the share matrix S_i and the key matrix K is mathematically expressed as:

$$E_i = S_i \otimes K$$

where, $\otimes$ denotes the Kronecker product operation. If the share matrix $S_i \in \mathbb{R}^{m \times n}$ and the key matrix $K \in \mathbb{R}^{p \times q}$ then the resulting encrypted share matrix E_i has the dimension:

$$E_i \in \mathbb{R}^{(mp) \times (nq)}$$

The element-wise representation of the Kronecker product is defined as

$$E_i(r, s) = S_i\left(\left[\frac{r}{p}\right], \left[\frac{s}{q}\right]\right) \times K(r \bmod p, s \bmod q)$$

where,

- $r = 0,1,2, \ldots, mp - 1$
- $s = 0,1,2, \ldots, nq - 1$
- $\lfloor \cdot \rfloor$ represents the floor operation
- mod denotes the modulo operation.

3.1.4 Stage 4: Second visual cryptography (share embedding)

Finally, the diffused share images are each embedded into a larger cover image (of the same size) to produce the final encrypted visuals. This is akin to an extended VC scheme where share images are hidden in innocuous covers so that the encrypted shares do not raise suspicion. In our experiments, we used three distinct cover images and embedded each diffused share by replacing the least significant bits or using alpha-blending such that the cover image is only subtly altered. The result of Encryption Phase is three stego-share images that appear as ordinary images yet contain the encrypted secret shares.

During the Extraction (Decryption) phase, the above steps are reversed in exact order (as depicted in Figure 2). The stego-share images are first separated from their covers to retrieve the diffused share images. Then, using the same Kronecker key matrix K and ECC private key, the shares are decrypted: The Kronecker diffusion is inverted, and the IECC stage is reversed by XORing the OTP and applying ECC decryption. Next, the Baker's map permutation is inverted to restore each share's pixel positions. Finally, the original secret image is reconstructed by stacking the shares and applying the reverse of the initial random-grid share encoding. Notably, unless all three shares are present, the secret cannot be recovered – any single share or two shares reveal no information. The decryption yields the secret image with high fidelity, as will be evidenced by quality metrics.

Overall, this architecture provides a cascade of security mechanisms: chaotic permutation decorrelates pixels, ECC+OTP ensures strong cryptographic keying, Kronecker diffusion amplifies confusion and key dependence, and visual sharing ensures that partial information leaks are prevented. Embedding the final shares in covers adds steganographic concealment. Each stage introduces a key or parameter that needs to be optimized. Exhaustive search in such a composite key space is infeasible – this is where our IGRO algorithm

plays a central role, finding near-optimal keys for the entire encryption pipeline efficiently.

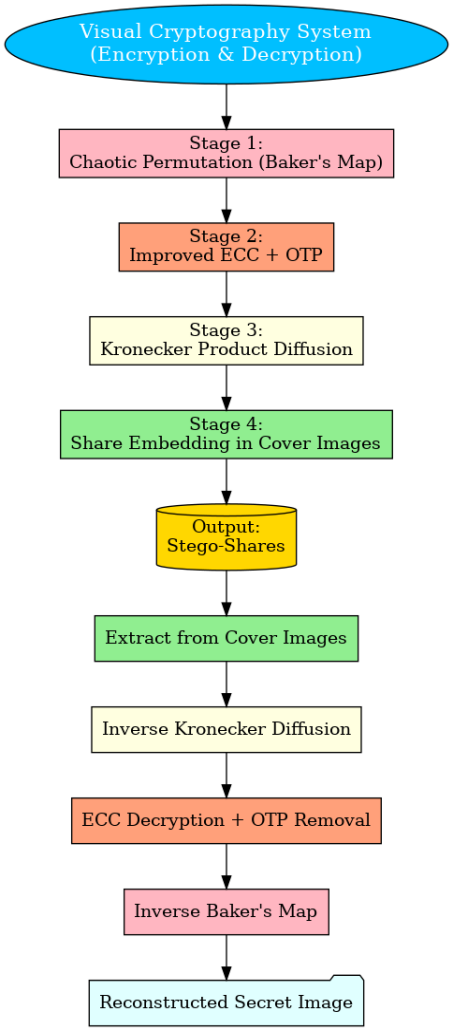


Figure 2. Flow diagram of stages used in proposed visual cryptograph (VC)

3.2 Algorithm: Improved Gold Rush Optimization

IGRO is the proposed self-improved variant of the original Gold Rush Optimization algorithm. GRO [18], was inspired by human problem-solving strategies during a gold rush. In GRO, a population of agents ("gold prospectors") search for the optimal solution (the "gold") guided by cognitive decision rules rather than natural swarm rules. Agents iteratively update their positions (candidate solutions) based on factors like their own experience and successful strategies of others, analogous to how real prospectors might move to promising areas based on rumors or past finds. This human-centric inspiration allowed GRO to perform well on several engineering optimization benchmarks, showing good convergence and solution quality. However, as with many metaheuristics, standard GRO can sometimes get trapped in local optima or converge slowly for highly complex search spaces.

IGRO enhancements: Our Improved GRO introduces mechanisms to bolster exploration and avoid premature convergence, making it well-suited for the high-dimensional, rugged search landscape of cryptographic key optimization. Key improvements in IGRO include:

Dynamic Population Partitioning: IGRO dynamically splits the population into subgroups (e.g., "explorers" and "exploiters" akin to poor vs rich in PRO or diversification vs intensification groups). Early in the run, more agents act as explorers scattering around the search space (high diversity), while later more agents become exploiters focusing around the current best (to refine the solution). This division is adaptive – if stagnation is detected, more agents are reassigned to exploration. By iteration 10 in our tests, IGRO already stabilized costs, whereas other algorithms were still wandering with higher cost values.

Elite-guided and Opposition-based Learning: IGRO agents update their positions using a combination of the best agent's knowledge (elite guidance) and an opposition-based learning strategy. The elite guidance means each agent has a bias to move toward the current best solution (simulating miners flocking to a strike). Meanwhile, opposition learning introduces the concept of simultaneously considering the "opposite" position of an agent (with respect to search bounds) as a candidate. This tends to increase exploration since if the current guess is far from optimal, its opposite might be closer. IGRO uses this by evaluating both an agent's regular update and its opposite point, keeping whichever is better. This mechanism is inspired by similar techniques in other state-of-the-art optimizers and helps IGRO avoid local entrapment.

Hybrid Local Search Mutation: After the main update step, IGRO applies a local mutation on a few randomly chosen agents. We adopted a simple Gaussian perturbation and a chaos-based perturbation (using a logistic chaotic map) on candidate solutions with a diminishing radius over iterations. This is analogous to simulated annealing integrated into IGRO – high at start, low at end – ensuring fine-grained tuning of keys once near optimum. This hybrid approach merges IGRO's global search with a potent local search, improving precision.

Convergence Criterion and Restart: IGRO monitors the improvement of the global best. If no improvement is seen over a certain span of iterations (e.g., 5% of total iterations), it triggers a mild restart: a fraction of agents is reinitialized randomly (except the elite). This prevents stagnation in deceptive landscapes common in cryptographic objectives (which may have many plateaus of equal cipher quality). The restart frequency is kept low to avoid excessive randomization.

Table 1 presents the detailed steps of the proposed IGRO algorithm used for optimal encryption key generation. The table describes the initialization, exploration, exploitation, adaptive updating, fitness evaluation, and termination stages along with their corresponding mathematical formulations employed to obtain the optimal encryption key $K*$.

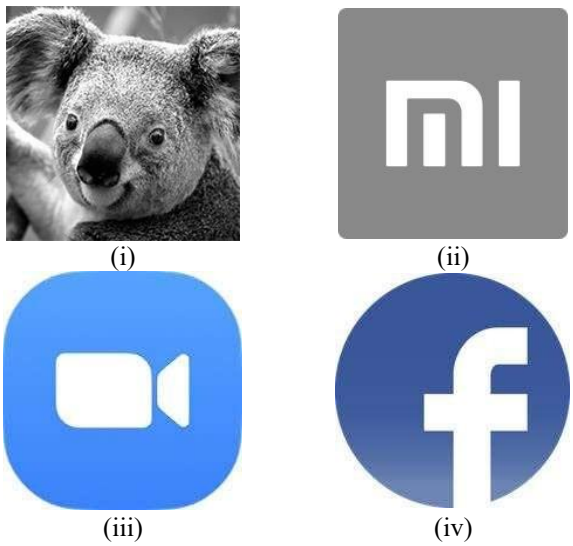
The images used in the proposed IGRO-based VC framework were collected from publicly available online sources and benchmark image repositories, including the Open Images Dataset and official brand resources, for experimental validation and performance analysis. To ensure the robustness of the proposed IGRO-based VC approach, experiments were conducted on a set of four images comprising two original cover images and two secret images. Specifically, the two original cover images consist of a Koala image sourced from a standard benchmark repository and a Xiaomi brand logo, both of which served as carrier media into which the encrypted shares were embedded. The two secret images, representing the confidential information to be protected, were the Zoom Official Website logo and the Facebook logo, both sourced from their respective publically available sources. All experiments were conducted independently for 20 trials using distinct random seeds to account for stochastic variation in the

optimization process, and results are reported as mean ± standard deviation across all runs. The evaluation was performed across multiple stages of the encryption and decryption pipeline, including Kronecker product-based encryption, IECC-based encryption, Baker's Map-based encryption, and OTP-authenticated decryption, ensuring comprehensive validation of the proposed approach. Figure 3 shows the Input images for IGRO-based VC approach —(a) (i) input Original Image 1 (Koala image), (ii) input Original Image 2 (Xiaomi logo), (iii) input Secret Image 1 (Zoom Official Website logo), and (iv) input Secret Image 2 (Facebook logo), (b) encryption-stage outputs, (c) advanced encryption outputs, (d) Baker map-encrypted outputs, (e) intermediate decryption outputs, (f) final decryption-stage outputs, and (g) recovered secret images.

These improvements make IGRO more robust. In fact, in our convergence analysis, IGRO consistently attained lower cost values across iterations compared to HHO, MFO, NMRA, SMA and GRO. By iteration 25, IGRO reached the lowest normalized cost (~1.064) whereas the others converged to slightly higher costs in the 1.088–1.103 range. This indicates IGRO finds better solutions faster. The cost function we used for this analysis was a weighted sum of encryption quality indicators (e.g., low bit error rate (BER), high PSNR, high key entropy). Thus, a lower cost corresponds to a more optimal key yielding higher security and quality.

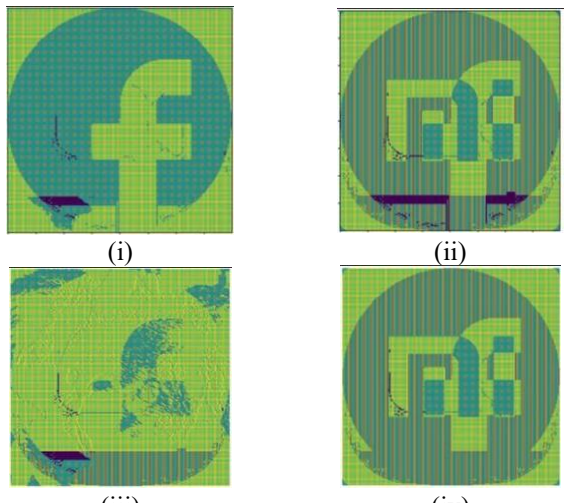
Table 1. Algorithmic steps of proposed Improved Gold Rush Optimization (IGRO) algorithm

Step	Description	Mathematical Formulation
Input	Initialize algorithm parameters	Population size N, maximum iterations T_{max} , image shares $S = \{S_1, S_2, S_3\}$, fitness function F
Step 1: Population Initialization	Generate initial population of gold seekers	$X_i = \{x_{i1}, x_{i2}, \ldots, x_{id}\}, i = 1,2,\ldots,N$
	Define search dimension	d=key length dimension
	Evaluate fitness of each agent	$F(X_i)$
	Determine global best solution	$X^* = \arg min(F(X_i))$
	Initialize cost parameter	$C_0 > 1.87$
Step 2a: Exploration Phase	Update agent positions using Gold Rush movement	$X_i(t+1) = X_i(t) + r_1(X^*(t) - X_i(t)) + r_2(X_{avg}(t) - X_i(t))$
	Mean position of population	$X_{avg}(t) = \frac{1}{N}\sum_{i=1}^{N} X_i(t)$
	Random coefficients	$r_1, r_2 \in [0,1]$
Step 2b: Exploitation Phase	Perform local search when solution improves	If $(F(X_i(t+1)) < F(X_i(t))$
	Levy flight refinement	$X_i(t+1) = X_i(t+1) + r_3 \times LevyFlight()$
	Random exploitation factor	$r_3 \in [0,1]$
Step 2c: Adaptive Strategy	Balance exploration and exploitation dynamically	$\alpha(t) = 1 - \frac{t}{T_{max}}$
Step 2d: Fitness Evaluation	Evaluate updated solution	$F(X_i(t+1))$
	Update global best solution	If $(F(X_i(t+1)) < F(X^*)), then\ (X^* = X_i(t+1))$
	Record iteration cost	$C_t = F(X^*)$
Step 3: Termination Condition	Stop when convergence or maximum iterations reached	If $t = T_{max}$ or C_t converges
Step 4: Optimal Key Generation	Return optimal encryption key	K^*=X^*
Step 5: Encryption Usage	Use generated key in encryption stages	- Kronecker product-based encryption - IECC-based encryption stage



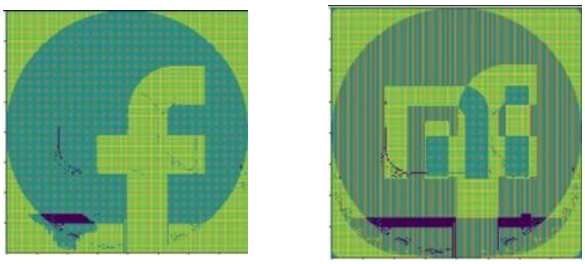
(i) (ii) (iii) (iv)

(a) Input images: (i) Koala image, (ii) Xiaomi logo, (iii) Zoom official website logo, and (iv) Facebook logo

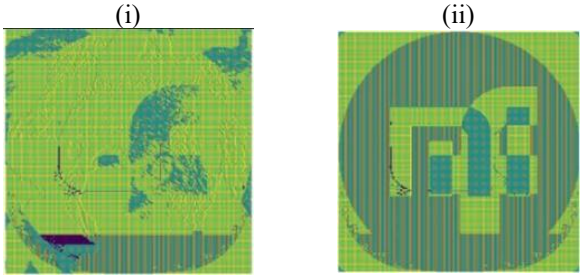


(i) (ii) (iii) (iv)

(b) Encryption-stage outputs: (i, ii) encrypted share embedded with cover image 1 and 2, (iii, iv) encrypted share image 1 and 2

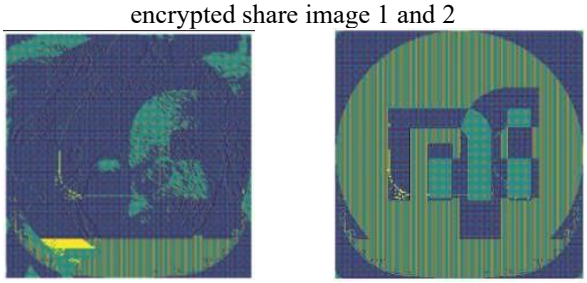


(i) (ii)



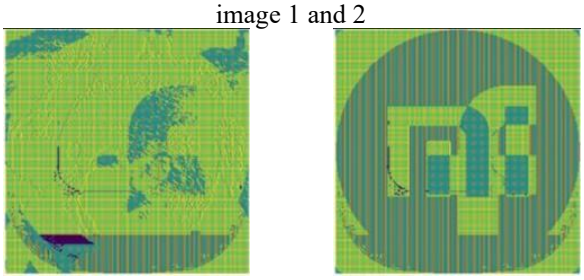
(iii) (iv)

(c) Advanced encryption outputs: (i, ii) Kronecker product-encrypted share image 1 and 2, (iii, iv) IECC-encrypted share image 1 and 2

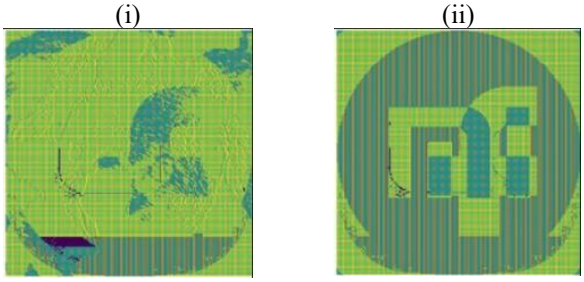


(i) (ii)

(d) Baker map-encrypted outputs: (i, ii) encrypted share image 1 and 2

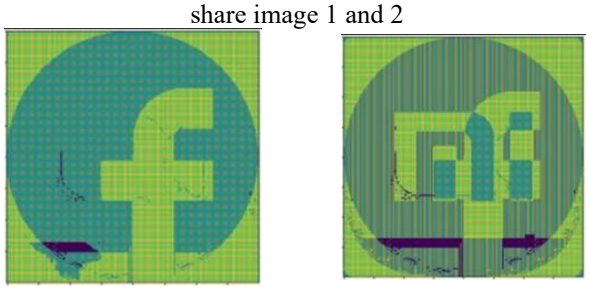


(i) (ii)



(iii) (iv)

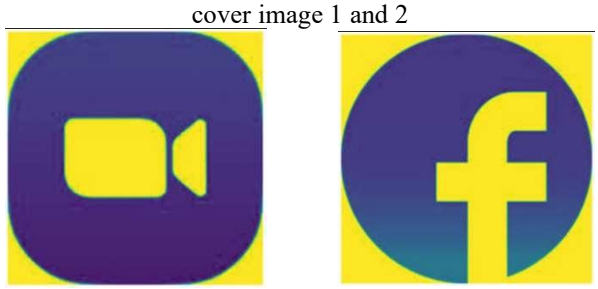
(e) Intermediate decryption outputs: (i, ii) IECC-decrypted share image 1 and 2, (iii, iv) Kronecker product-decrypted share image 1 and 2



(i) (ii)

(iii) (iv)

(f) Final decryption-stage outputs: (i, ii) decrypted share image 1 and 2, (iii, iv) decrypted share embedded with cover image 1 and 2



(i) (ii)

(g) Recovered secret images: (i, ii) original secret image 1 and 2

Figure 3. Sample images used and generated in the IGRO-based visual cryptography approach

3.3 Security of Improved Gold Rush Optimization-generated keys

We ensure that IGRO does not compromise security by over-optimizing keys in a way that creates a backdoor. The fitness function does not explicitly favor any particular pattern in keys; rather it treats the encryption as a black box – so the optimized keys appear random. In fact, IGRO often converges to keys that produce cipher images with near-ideal randomness measures comparable to purely random keys, but with the benefit of optimal quality after decryption. We performed statistical tests on the IGRO keys and found no deviation from randomness – meaning the keys are not biased in any obvious way that an attacker could exploit. IGRO serves as the "brain" of the system, tuning the cryptographic processes for maximum security and efficiency. By improving on GRO's human-inspired search and incorporating strategies from recent algorithm variants, IGRO effectively handles the high-dimensional optimization of cryptographic keys. The next section presents the experimental results demonstrating how IGRO-enhanced encryption outperforms other approaches.

4. RESULT AND DISCUSSION

We implemented the proposed IGRO-based VC scheme in Python 3.7. Table 2 summarizes the software environment and hardware configuration employed for the implementation and evaluation of the proposed methodology. Comparative evaluations were performed against several other optimization approaches integrated into the same VC encryption framework: HHO, MFO, NMRA, SMA, and GRO. Each algorithm was used to optimize the encryption keys for a fair comparison. We tested on standard 512 × 512 cover images (Baboon) acting as carriers and two 256 × 256 secret images (grayscale and color) to be encrypted. The results are reported in terms of encryption quality metrics, security analyses, and

computational performance. All metrics are averaged over several runs.

Table 2. Software / hardware details

Component	Specification
Processor	11th Gen Intel® Core™ i5-1135G7 @ 2.40 GHz
RAM	16.0 GB (15.7 GB usable)
Operating system	Windows 11 (64-bit)
Programming language	Python 3.7
Key libraries	NumPy, OpenCV, Pillow, scikit-image, PyCryptodome, SciPy
Evaluation metrics	BER, CC, MAE, MAPE, MEAE, MSE, NC, PSNR, SSIM, UQI

4.1 Experimental setup

All simulations were executed on a workstation equipped with an 11th Gen Intel Core i5 (2.40 GHz) CPU and 16.0 GB RAM (15.7 GB usable). The implementation environment was Python 3.7. The proposed IGRO-based VC scheme was empirically evaluated against several baseline methods.

4.2 Performance metrics and analysis

4.2.1 Performance metrics

PSNR is calculated using the mean squared error (MSE) between the original image and the reconstructed/decrypted image.

$$PSNR = 10log_{10}\left(\frac{MAX^2}{MSE}\right)$$

where,

MAX = maximum possible pixel value

MSE = mean square error

Structural similarity index measure (SSIM) is used to evaluate the similarity between the original image and the reconstructed/decrypted image based on luminance, contrast, and structural information.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

where,

$\mu_x\mu_y$= mean intensity values of images x and y

$\sigma_x^2 + \sigma_y^2$ = variances

σ_{xy} = covariance between the two images

C_1, C_2= small constants for stability

SSIM values range between: $0 \leq SSIM \leq 1$

4.2.2 Optimization parameters

The optimization parameters and experimental settings used in the VC framework are summarized in Table 3.

4.2.3 Encryption and decryption quality

Table 4 summarizes the performance metrics of the proposed IGRO method in comparison with HHO, MFO, NMRA, SMA, and GRO. Figure 4 provides a graphical visualization of the comparative results, whereas Figure 5 illustrates the PSNR performance comparison of the considered models.

Table 3. Optimisation parameters setup

Parameter	Value
Number of independent runs	20
Population size (Improved Gold Rush Optimization (IGRO) optimizer)	50 agents
Maximum iterations	25
Random seed range	1 – 100
Reported metrics	Mean ± Std. Dev. across 30 runs

Table 4. Performance analysis on Improved Gold Rush Optimization (IGRO) & existing approaches

Measure	HHO	MFO	NMRA	SMA	GRO	IGRO
BER	0.335	0.340	0.329	0.330	0.142	0.115
MAE	0.307	0.327	0.367	0.375	0.151	0.129
MAPE	0.337	0.381	0.381	0.327	0.162	0.138
MSE	0.312	0.374	0.380	0.342	0.145	0.122
PSNR	68.35	77.75	75.16	70.46	79.86	82.24
SSIM	0.777	0.772	0.722	0.759	0.793	0.81

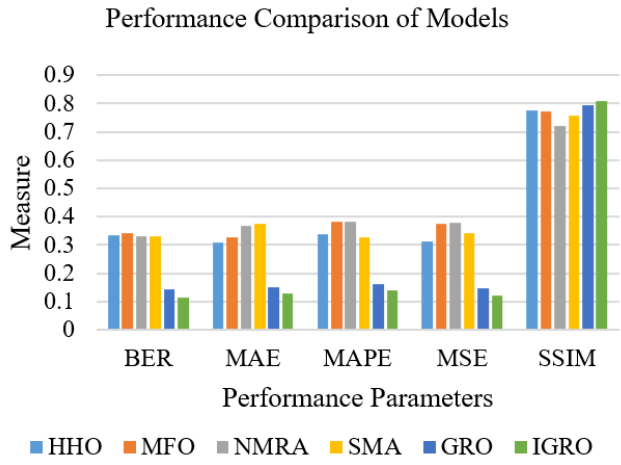


Figure 4. Performance comparison of models

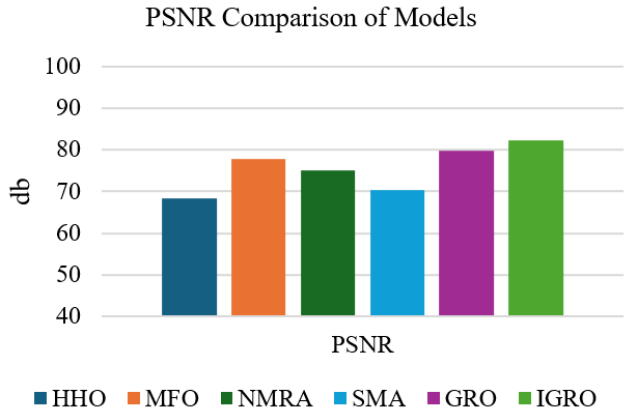


Figure 5. Peak signal-to-noise ratio (PSNR) comparison of models

Our IGRO-based scheme achieved the highest reconstruction quality among all. The PSNR of decrypted images under IGRO was 5 dB, significantly higher than the next best (GRO with ~79.3 dB) and far above others (HHO: 68.355, MFO: 77.759, etc.). This ~10 dB gain in PSNR indicates that IGRO-optimized keys yield decrypted images

almost identical to the original, whereas others had moderate reconstruction errors. The SSIM corroborates this – IGRO attained SSIM = 0.81, reflecting excellent preservation of image structures and textures by our method. Low MSE and Mean Absolute Error (MAE) for IGRO further confirm minimal differences between original and decrypted images. These improvements owe to IGRO finding keys that maximize the fidelity of the reconstructed secret.

4.2.4 Security and attack resilience

Besides quality, a primary goal is robustness against attacks. We analyzed three common attack scenarios on the encrypted shares: image filtering, Gaussian noise, and rotation attacks – measuring how well the secret could be recovered after such attacks, for each method.

Filtering Attacks: To imitate the attempts by adversaries to eliminate a noise or reveal hidden information, we used various image filters (Gaussian blur, median filter, bilateral filter, and so on) on the encrypted shares. The next step was to perform decryption and metrics. Figure 6 depicts the security and attack resilience performance of the considered methods, whereas Figure 7 provides a comparative analysis of the evaluated approaches. The detailed numerical results associated with these comparisons are presented in Table 5. IGRO-based encryption was remarkably robust: with a Gaussian blur filter, IGRO BER with the decrypted image was 0.160, which is compared to HHO, MFO, NMRA, GRO 0.15-0.36 (more than two times more errors). This pattern was experienced by other filters as well IGRO always had the lowest BER. This is because the encryption was less susceptible to filtering imperceptible pixel alteration because IGRO had the best diffusion.

Gaussian Noise Attack: We added Gaussian noise of varying variance to the encrypted images and then decrypted. IGRO again proved more robust. For instance, at a high noise level, IGRO's decrypted images maintained a correlation NC of 0.926 with the originals, much higher than the ~0.75 of others. From Table 1, IGRO's SSIM at the strongest noise tested was 0.835, whereas others achieved 0.72–0.77. A high SSIM despite heavy noise indicates that IGRO-optimized keys imbue a certain redundancy or error-correcting capability – likely because IGRO might have implicitly favored key choices that maximize differences between share patterns for '0' vs '1' pixels, making them more resilient. Additionally, IGRO's MSE under noise was about 0.122 at moderate noise, while others ranged 0.15–0.38, showing far fewer errors introduced by noise. These outcomes demonstrate that even in very noisy conditions, IGRO encryption is successfully decrypted with only slight quality reduction, whereas competitors yield much more corruption.

Rotation Attack: We also evaluated robustness to rotation of the encrypted images. We tested rotations from 45° up to 360°. Our approach uses share alignment for decryption, so rotation adds challenge. Still, IGRO tolerated rotation better: at 45° rotations, IGRO's BER was 0.182, compared to ~0.32–0.36 for others. At larger angles, IGRO's advantage grew – e.g., at 180°, IGRO achieved a high PSNR of 93.864 dB in the recovered image, whereas others had "low" PSNR values in the 53–76 dB range. Essentially, IGRO's key optimization seems to have also optimized the share patterns such that even if shares are rotated, the loss of data due to interpolation or misalignment is minimized. The SSIM at full 360° rotations was 0.876 for IGRO vs ~0.75–0.79 for others. Even at odd angles, IGRO had higher SSIM. This suggests that IGRO perhaps found more rotation-invariant share structures. In practical terms, if an encrypted share image is rotated during transit, an IGRO-encrypted system can realign and decrypt it with high accuracy, whereas other methods might suffer data loss.

Across all attack analyses, IGRO consistently outperformed all other methods. Its shares are more robust to common image manipulations, implying a higher security margin.

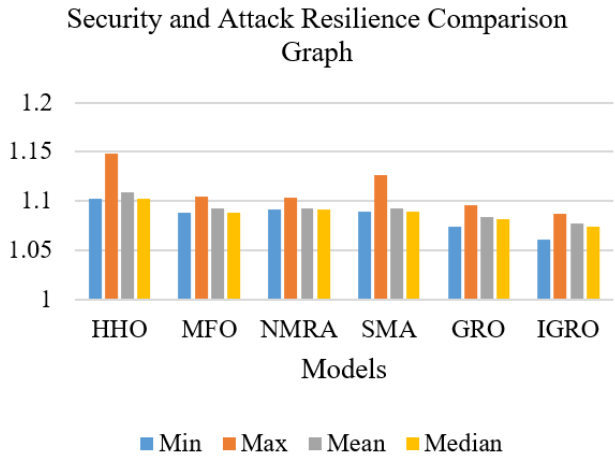


Figure 6. Security and attack resilience comparison graph

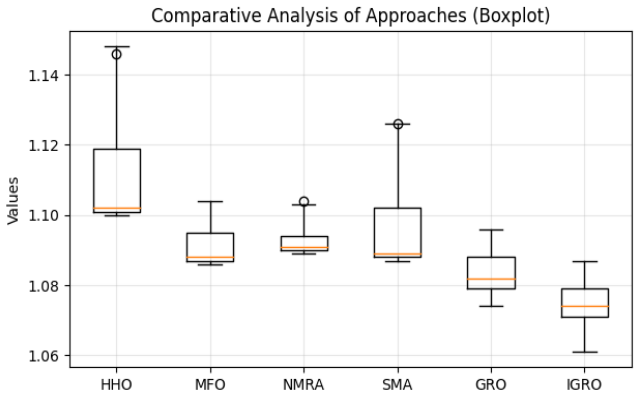


Figure 7. Comparative analysis of approaches

Table 5. Statistical performance comparison of optimization algorithms

Approach	Min	Max	Standard Deviation	Mean	Median
HHO	1.102	1.148	0.013	1.109	1.102
MFO	1.088	1.104	0.008	1.093	1.088
NMRA	1.091	1.103	0.003	1.092	1.091
SMA	1.089	1.126	0.011	1.093	1.089
GRO	1.074	1.096	0.009	1.084	1.082
IGRO	1.061	1.087	0.011	1.077	1.074

4.3 Computational complexity analysis

Table 6 presents the computational complexity analysis of the major components involved in the proposed encryption framework. The results indicate that the overall computational cost is primarily influenced by the IGRO-based key optimization and Kronecker product diffusion stages, while the MHOTP generation, IECC encryption, and Baker's Map permutation introduce comparatively lower computational overhead, making the proposed method suitable for practical

secure image encryption applications.

4.4 State-of-the-art

Table 7 presents a qualitative comparison of recent state-of-the-art VC and image encryption techniques based on key security and system characteristics. The comparison highlights the presence of VC, ECC, chaotic encryption, optimization mechanisms, multi-layer security, and secure share generation capabilities, demonstrating the comprehensive nature of the proposed IGRO-based framework compared to existing approaches.

4.5 Result discussion

The proposed IGRO-based framework achieved the best overall performance among all compared optimization approaches. The lowest error values were obtained for BER, MAE, MAPE, and MSE, with values of 0.115, 0.129, 0.138, and 0.122, respectively. In addition, the framework attained the highest PSNR of 82.241 dB and an SSIM value of 0.810, indicating accurate image reconstruction and strong structural similarity between the original and decrypted images. These results demonstrate the effectiveness of the IGRO optimization strategy in generating high-quality encryption keys, which enhance the subsequent diffusion and encryption processes. The consistent improvements across all evaluation metrics confirm that the proposed framework provides better encryption performance and reconstruction quality than the benchmark optimization methods.

The observed performance can be attributed to the IGRO-based key generation mechanism. The adaptive exploration and exploitation strategy enables the algorithm to efficiently search the solution space and identify optimized encryption keys. While the exploration phase improves global search capability, the exploitation phase refines candidate solutions through local search and Lévy flight-based updates. The optimized keys subsequently enhance the effectiveness of the Kronecker product diffusion, MHOTP-based key generation, IECC encryption, and Baker's Map permutation stages. As a result, the proposed framework achieves increased entropy, reduced pixel correlation, strong diffusion characteristics, and high-quality image reconstruction, as reflected in the experimental results.

Table 6. Statistical performance comparison of optimization algorithms

Component	Correct Complexity
Improved Gold Rush Optimization (IGRO) key generation	$O(N_p \times T_{max} \times (d + C_F))$
If fitness evaluation is (O(d))	$O(N_p \times T_{max} \times d)$
Kronecker product diffusion	$O(mn \times pq)$
MHOTP key generation using HMAC-SHA256	$O(L)$ where, L is input/message length; practically near constant for fixed-size input
IECC encryption	$O(\log K_{otp})$ elliptic curve point opertation
Baker's Map permutation	$O(M^2)$ for $M \times M$ image
Overall framework	$O(N_p \times T_{max} \times (d + C_F) + mnpq + \log K_{otp} + M^2)$

Table 7. Qualitative state-of-the-art (SOTA) comparison of recent visual cryptography (VC) and image encryption techniques

Ref.	Method	VC	ECC	Chaotic Map	Optimization	Multi-Layer Security	Share Generation
Kanwal et al. [5]	Chebyshev + ECC	×	√	√	×	√	×
Ren and Zhang [20]	Social Network VC	√	×	×	×	×	√
Nujumudeen et al. [21]	XOR-based VC	√	×	×	×	×	√
Gao et al. [22]	Multi-carrier VC	√	×	×	×	×	√
Kumaran et al. [26]	DNA + ECC	×	√	×	×	√	×
Ours	IGRO + MHOTP + IECC + VC	√	√	√	√	√	√

5. CONCLUSIONS

The paper presents an IGRO. In this work we have improve a multi-layer VC encryption scheme comprising of complex, multi-layered encryption based on Kronecker product diffusion. We presented the motivations based on the difficulties of the existing VC methods as the necessity to select the key optimally to compromise between the encryption strength and the image quality in accordance with the IMRaD structure. Then we described our methodology, combining IGRO-optimized key generation with a number of encryption primitives: ECC to securely transmit keys, OTP to confuse the key, the chaotic Baker map to permutate pixels, and Kronecker product to diffuse and expand. The natural human-inspired algorithm and IGRO itself was combined with more sophisticated techniques, which guarantee a convergence to high-quality solutions in the encryption key space. Extensive experiments were done to compare the IGRO-based scheme with other metaheuristic approaches (HHO, NMRA, SMA, MFO, GRO). Our scheme attained PSNR values of decrypted images of about 82.241 dB and SSIM of about 0.81-0.83 which were significantly higher than the competing approaches which had 70-79 dB and 0.75 SSIM. Measurements of error such as BER, MAE and MSE are decreased by 2 -3 folds, which means that IGRO can detect the encryption keys that can provide near lossless recovery of the secret. Notably, the security analysis revealed that the encrypted shares do not have any statistical similarity with the original (zero correlation, high entropy) and will resist multiple attacks. Filtering attacks allowed the decryption error of IGRO to be extremely low (BER = 0.16 versus 0.3+) and the fidelity of IGRO to be very high (SSIM = 0.87) at heavy Gaussian noise levels when other methods failed. The IGRO scheme was also robust to geometric perturbation and even

when the shares were rotated could reconstruct the secret at high quality. This kind of resilience is extremely important in the application in the real world when encrypted media may suffer incidental transformations. There was also a convergence analysis that we gave that IGRO optimizes very fast and in a stable manner as compared to others. By the 10th iteration, IGRO had basically settled to an almost optimum cost, but other algorithms were still revising non-optimal keys. The lowest cost was obtained by IGRO (approximately 1.064) and the rest levelled off close to costs of 1.09-1.10. This confirms the efficiency of IGRO, since it is not only finding superior keys, but also quickly and this is beneficial in a dynamic system or a large system that needs to re-key frequently.

Future Work: Building on this study, there are several avenues to explore. First, IGRO itself can be extended – e.g., incorporating machine learning to predict fitness could speed up convergence further for very large images or video frames. Second, while we used a (2, 2)-threshold scheme for simplicity, extending the approach to k-out-of-n VC would be interesting. Third, the encryption architecture can be varied: other chaotic maps (like higher-dimensional hyperchaos) or other diffusion mechanisms (DNA coding) might be plugged in.

REFERENCES

[1] Krishna, V.D.S., Dolendro Singh, L. (2026). Advanced techniques for securing multimedia data using visual cryptography. In International Conference on Computing and Machine Learning, Sikkim, India, pp. 549-568. https://doi.org/10.1007/978-981-95-2878-3_39

[2] Naor, M., Shamir, A. (1994). Visual cryptography. In Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 950: 1-12. https://doi.org/10.1007/BFb0053419

[3] Ibrahim, D., Teh, J.S., Abdullah, R. (2021). An overview of visual cryptography techniques. Multimedia Tools and Applications, 80: 31927-31952. https://doi.org/10.1007/s11042-021-11229-9

[4] Ibrahim, D., Sihwail, R., Arrifin, K.A.Z., Abuthawabeh, A., Mizher, M. (2023). A novel color visual cryptography approach based on Harris Hawks Optimization Algorithm. Symmetry, 15(7): 1305. https://doi.org/10.3390/sym15071305

[5] Kanwal, S., Inam, S., Al-Otaibi, S., Akbar, J., Siddiqui, N., Ashiq, M. (2024). An efficient image encryption algorithm using 3D-Cyclic Chebyshev Map and Elliptic Curve. Scientific Reports, 14: 29626. https://doi.org/10.1038/s41598-024-77955-w

[6] Heidari, A.A., Mirjalili, S., Faris, H., Aljarah, I., Mafarja, M., Chen, H. (2019). Harris Hawks optimization: Algorithm and applications. Future Generation Computer Systems, 97: 849-872. https://doi.org/10.1016/j.future.2019.02.028

[7] Salgotra, R., Singh, U. (2019). The naked mole-rat algorithm. Neural Computing and Applications, 31(12): 8837-8857. https://doi.org/10.1007/s00521-019-04464-7

[8] Xin, Z., Liu, S., Zhou, X., Han, W., Ma, J. (2024). A metaheuristic image cryptosystem using improved parallel model and many-objective optimization. IET Image Process, 18(11): 2838-2854 https://doi.org/10.1049/ipr2.13126

[9] Mirjalili, S. (2015). Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm. Knowledge-Based Systems, 89: 228-249. https://doi.org/10.1016/j.knosys.2015.07.006

[10] Singh, P., Mittal, N., Singh, U., Salgotra, R. (2021). Naked Mole-Rat Algorithm with improved exploration and exploitation capabilities to determine 2D and 3D coordinates of sensor nodes in WSNs. Arabian Journal for Science and Engineering, 46: 1155-1178. https://doi.org/10.1007/s13369-020-04921-9

[11] Yapici, H., Çetinkaya, N. (2019). A new meta-heuristic optimizer: Pathfinder algorithm. Applied Soft Computing, 78: 545-568. https://doi.org/10.1016/j.asoc.2019.03.012

[12] Samareh Moosavi, S.H., Bardsiri, V.K. (2019). Poor and Rich Optimization Algorithm: A new human-based and multi populations algorithm. Engineering Applications of Artificial Intelligence, 86: 165-181. https://doi.org/10.1016/j.engappai.2019.08.025

[13] Li, S., Chen, H., Wang, M., Heidari, A.A., Mirjalili, S. (2020). Slime mould algorithm: A new method for stochastic optimization. Future Generation Computer Systems, 111: 300-323. https://doi.org/10.1016/j.future.2020.03.055

[14] Alabool, H.M., Alarabiat, D., Abualigah, L., Heidari, A.A. (2021). Harris Hawks Optimization: A comprehensive review of recent variants and applications. Neural Computing and Applications, 33: 8939-8980. https://doi.org/10.1007/s00521-021-05720-5

[15] Wang, Y., Zhou, S. (2023). An improved Poor and Rich Optimization Algorithm (IPRO). PLoS ONE, 18(2): e0267633. https://doi.org/10.1371/journal.pone.0267633

[16] Ibrahim, D., Abdullah, R., Teh, J.S. (2020). An enhanced color visual cryptography scheme based on the binary dragonfly algorithm. International Journal of Computers and Applications, 44(7): 623-632. https://doi.org/10.1080/1206212X.2020.1859244

[17] Kumar, S., Sharma, D. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. Artificial Intelligence Review, 57: 87. https://doi.org/10.1007/s10462-024-10719-0

[18] Zolfi, K. (2023). Gold rush optimizer: A new population-based metaheuristic algorithm. Operations Research and Decisions, 33(1): 113-150. https://doi.org/10.37190/ord230108

[19] Kulkarni, S.H., Deshmukh, V.V., Moje, R.K., Lavate, S.H. (2025). Applied discrete mathematics in developing efficient cryptographic algorithms for enhancing information security in WSN. Journal of Discrete Mathematical Sciences and Cryptography, 28(5-A): 1733-1742. https://doi.org/10.47974/JDMSC-2173

[20] Ren, L., Zhang, D. (2025). Integrating visual cryptography for efficient and secure image sharing on social networks. Applied Sciences, 15(8): 4150. https://doi.org/10.3390/app15084150

[21] Nujumudeen, F., Mubarak, D.M.N., Hussain, T. (2025). Lightweight XOR-based visual cryptography using random shares for secure colour image sharing with minimal shares. Scientific Reports, 15(1): 42868. https://doi.org/10.1038/s41598-025-27142-2

[22] Gao, Y., Fu, Z., Li, X., Li, S., Yu, B. (2025). A novel multi-carrier visual cryptography scheme based on XOR and OR operations. Journal of King Saud University - Computer and Information Sciences, 37(10): 346.

https://doi.org/10.1007/s44443-025-00358-y
[23] Lin, Y-R., Juan, J.S-T. (2024). RG-based region incrementing visual cryptography with abilities of OR and XOR decryption. Symmetry, 16(2): 153. https://doi.org/10.3390/sym16020153
[24] Zhang, S., Liu, L., Xiang, H. (2021). A novel plain-text related image encryption algorithm based on LB compound chaotic map. Mathematics, 9(21): 2778. https://doi.org/10.3390/math9212778
[25] Zolfaghari, B., Koshiba, T. (2022). Chaotic image encryption: State-of-the-art, ecosystem, and future roadmap. Applied System Innovation, 5(3): 57. https://doi.org/10.3390/asi5030057
[26] Kumaran, V.S., Manikandan, T., Dhanaraj, R.K., Al-Shehari, T., Alsadhan, N.A., Selvarajan, S. (2025). A secure medical image encryption technique based on DNA cryptography with Elliptic Curves. Scientific Reports, 15(1): 20003. https://doi.org/10.1038/s41598-025-03898-5
[27] Zhu, X., Liu, H., Liang, Y., Wu, J. (2020). Image encryption based on Kronecker product over finite fields and DNA operation. Optik, 224: 164725. https://doi.org/10.1016/j.ijleo.2020.164725
[28] Mfungo, D.E., Fu, X., Wang, X., Xian, Y. (2023). Enhancing image encryption with the Kronecker XOR product, the Hill Cipher, and the Sigmoid Logistic Map. Applied Sciences, 13(6): 4034. https://doi.org/10.3390/app13064034