International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(20s) 2026 pp. 549-557
https://doi.org/10.70917/ijcisim-2026-5166
Article

A Hybrid Chaos–AES–Visual Cryptography Framework with Burrows–Wheeler Transform-Based Compression for Secure and Efficient Image Transmission

V.Senthil Balaji[1], Dr.R.Priya[2], Dr.V.Punitha[3]

[1]Research Scholar Department of Computer Science Engineering FEAT Annamalai University Chidambaram, Tamilnadu, India
senthilvvrvv@gmail.com
[2]Professor Department of Computer Science Engineering FEAT Annamalai University Chidambaram, Tamilnadu, India
pryknd n@yahoo.com
[3]Professor and Head Department of Computer Science Engineering Saranathan college of Engineering , Tiruchirapalli, India
cse.hod@saranathan.ac.in

Abstract: Secure transmission of digital images over open networks requires encryption schemes that balance security, efficiency, and bandwidth utilization. This paper presents a hybrid image transmission framework that integrates Burrows–Wheeler Transform (BWT) based lossless compression with chaos-assisted AES encryption and visual cryptography. The input image is first compressed to reduce redundancy and transmission overhead. A chaotic map is then employed for sensitive key generation and permutation, followed by AES encryption to ensure strong diffusion characteristics. To further enhance transmission security, the encrypted data is divided into multiple shares using a visual cryptography scheme, ensuring that individual shares reveal no meaningful information. Authorized reconstruction is possible only with correct cryptographic keys and valid shares. Experimental evaluation demonstrates high entropy, low correlation, strong resistance to statistical and differential attacks, and acceptable computational complexity, confirming the suitability of the proposed scheme for secure image transmission.
Keywords: Image encryption; Secure image transmission; Burrows–Wheeler transform; Chaos-based encryption; Advanced Encryption Standard (AES); Visual cryptography; Lossless compression; Cryptographic security.

1. Introduction

The secure exchange of digital images has become increasingly important as visual data is widely transmitted across open networks in modern communication systems. Images are commonly used in domains such as medical diagnosis, remote surveillance, biometric identification, cloud-based services, and multimedia applications, where unauthorized access or data leakage can lead to serious consequences. As a result, developing reliable techniques for protecting image data during transmission remains a significant research challenge.

Standard encryption algorithms, including the Advanced Encryption Standard (AES), are extensively used to secure textual information due to their strong cryptographic foundations. However, when these algorithms are directly applied to image data, their efficiency is often limited. Digital images typically contain a large amount of redundant information and exhibit strong correlation among neighboring pixels, which reduces the effectiveness of conventional encryption approaches and increases computational overhead.

In recent years, chaos-based encryption techniques have been explored as an alternative solution for image security. Chaotic systems exhibit nonlinear behaviour, pseudo-random characteristics, and high sensitivity to initial conditions, which make them suitable for cryptographic key generation and permutation operations. These properties

enable effective scrambling of image data; however, chaos-based schemes used independently may not provide sufficient diffusion and can be vulnerable to cryptanalytic attacks.

To address these limitations, hybrid encryption schemes that combine chaos-based techniques with AES have been proposed. In such approaches, chaotic maps are commonly used to enhance key sensitivity and permutation, while AES contributes strong diffusion and resistance to brute-force attacks. Although this combination improves security, it does not inherently address the redundancy present in image data, and the computational cost may increase when encrypting large images.

Visual cryptography (VC) introduces an additional security mechanism by dividing encrypted data into multiple shares, where each share individually contains no meaningful information. Image reconstruction is possible only when a predefined number of valid shares are combined. This property makes VC particularly suitable for distributed and multi-user environments; however, due to pixel expansion and structural constraints, VC is generally employed as a supplementary security layer rather than a standalone encryption technique.

In parallel, data compression has been recognized as an effective means to improve transmission efficiency. Lossless compression methods, such as the Burrows–Wheeler Transform (BWT), reduce data redundancy without affecting image quality. Performing compression prior to encryption not only reduces bandwidth requirements but also improves encryption efficiency by operating on a less redundant data representation.

Motivated by these observations, this paper proposes a hybrid secure image transmission scheme that integrates Burrows–Wheeler compression, chaos-based encryption, AES, and visual cryptography. The proposed framework first applies BWT-based lossless compression to minimize redundancy, followed by chaotic key generation and permutation to enhance sensitivity. AES is then used to ensure strong cryptographic diffusion, and visual cryptography is employed to enable secure share-based transmission. Experimental results demonstrate that the proposed scheme provides high security, efficient bandwidth utilization, and strong resistance against statistical and differential attacks, making it suitable for secure image transmission in modern communication environments.

2. Literature Survey

Secure image transmission has received sustained research attention due to the inherent characteristics of digital images, including high redundancy, strong spatial correlation among pixels, and large data volumes. Conventional cryptographic algorithms designed for textual data are often inefficient when directly applied to image data, motivating the development of image-specific encryption schemes [1]. A comprehensive review of existing image encryption techniques, covering spatial-domain, transform-domain, and hybrid approaches, highlights the need for improved trade-offs between security strength and computational efficiency [1].

Chaos-based cryptographic systems have been widely explored because of their sensitivity to initial conditions, pseudo-randomness, and erotic behaviour, which align well with fundamental cryptographic requirements. Alvarez and Li established essential design criteria for chaos-based cryptosystems, emphasizing key sensitivity, diffusion capability, and resistance to statistical attacks [2]. Building on these principles, Wu et al. proposed a colour image encryption scheme that integrates DNA encoding with spatiotemporal chaotic systems, achieving enhanced confusion and diffusion properties [3]. Similarly, Liu et al. introduced a chaos-driven image encryption algorithm with a symmetric diffusion structure, demonstrating improved robustness against differential attacks [4].

Standard block ciphers, particularly the Advanced Encryption Standard (AES), have also been adapted for image encryption due to their proven security and wide acceptance. Nahta et al. investigated simple and modified AES-based image encryption techniques, reporting improved security performance but increased computational overhead for high-resolution images [5]. To address such limitations, hybrid encryption schemes combining substitution–permutation networks with chaotic maps were proposed, enhancing nonlinearity while maintaining acceptable computational efficiency [6].

Visual cryptography (VC) offers a distinct security paradigm by dividing secret information into multiple shares, such that individual shares do not reveal meaningful information. The foundational visual cryptography model introduced by Naor and Shamir demonstrated secure image sharing without complex cryptographic computations [7]. Subsequent research extended this concept to support multiple secret images [8] and colour image encryption using random grid techniques, improving applicability in practical multimedia systems [9]. Despite these advantages, visual cryptography schemes often suffer from pixel expansion and reconstruction quality degradation.

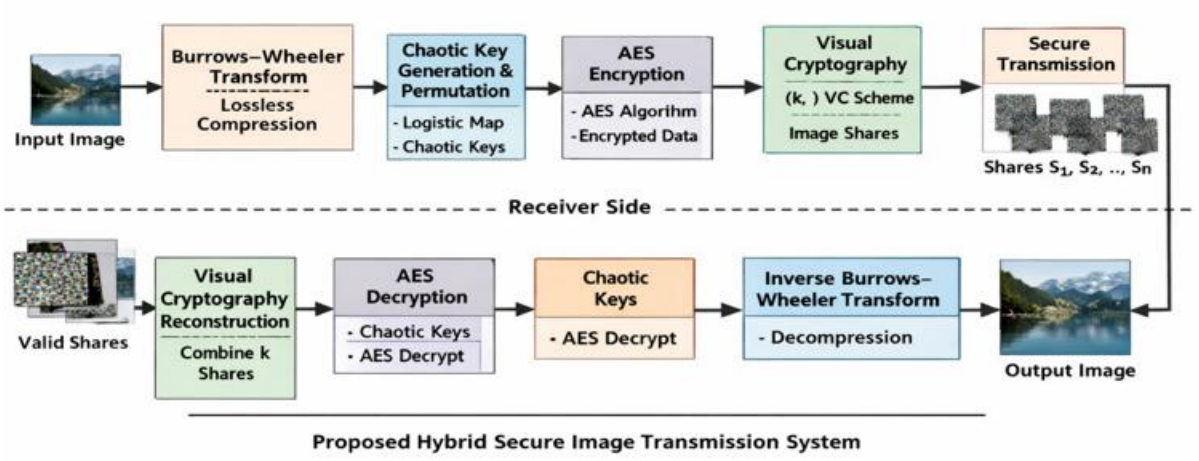
To improve bandwidth efficiency and reduce transmission overhead, lossless compression techniques have been incorporated into secure image transmission systems. The Burrows–Wheeler Transform (BWT) reorganizes data to enhance compressibility while preserving information content [10]. Comparative studies on lossless compression methods confirm their effectiveness in reducing redundancy prior to encryption [11], [12]. Integrating compression with encryption has been shown to improve both security and efficiency. Jolfaei proposed a secure image transmission approach combining chaos-based encryption with compression [13], while Zhang et al. presented a joint compression–encryption framework aimed at secure and efficient image transmission over public networks [14].

Classical compression algorithms such as the Lempel–Ziv method further emphasize the importance of redundancy reduction in data transmission systems [15]. However, existing studies primarily focus on partial integrations of encryption or compression techniques. Comprehensive multi-layer frameworks that simultaneously combine chaos-based encryption, standardized block ciphers, visual cryptography, and advanced lossless compression remain relatively underexplored in the literature.

3. Proposed Work

This work proposes a hybrid secure image transmission framework that integrates Burrows–Wheeler Transform (BWT)–based lossless compression, chaos-assisted AES encryption, and visual cryptography to achieve enhanced security, robustness, and transmission efficiency. The proposed system is designed to address the limitations of existing approaches by combining standardized cryptographic strength with chaos-driven randomness and share-based protection in a unified architecture.

In the proposed scheme, the input image is first subjected to lossless compression using BWT to reduce data redundancy and minimize transmission overhead without affecting image fidelity. Compression is performed prior to encryption to improve efficiency and to increase resistance against statistical attacks by altering data distribution. The compressed output is then prepared for cryptographic processing.



3.1 Choas Based Encryption

A chaotic map is employed to generate highly sensitive secret parameters and pseudo-random sequences. Due to the inherent sensitivity of chaotic systems to initial conditions, even minor variations in control parameters result

in significantly different encryption outcomes. These chaotic sequences are utilized for dynamic key generation, permutation control, and initial apparent diffusion, thereby enhancing key space and unpredictability.

3.2 AES Encryption

Following chaos-based pre-processing, the compressed data is encrypted using the Advanced Encryption Standard (AES). AES provides strong confusion and diffusion properties through multiple rounds of substitution, permutation, and key mixing operations. In the proposed framework, chaos-derived keys and permutations are incorporated into the AES process, strengthening resistance against brute-force, statistical, and known-plaintext attacks while retaining the reliability and security guarantees of a standardized block cipher.

3.2 Encryption using Visual Cryptography

To further enhance transmission security, the AES-encrypted image data is processed using a **(k,n)(k,n)(k,n)** visual cryptography scheme, where the encrypted image is divided into multiple independent shares. Each share appears noise-like and reveals no meaningful information individually. Secure reconstruction of the encrypted image is possible only when a sufficient number of authorized shares are combined, ensuring protection against data interception and unauthorized access during transmission.

At the receiver side, the reverse operations are performed in sequence. Authorized shares are combined to reconstruct the encrypted image, followed by AES decryption using the correct chaotic parameters and secret keys. The decompressed image is finally recovered through inverse BWT, resulting in a lossless reconstruction of the original image.

The proposed hybrid framework offers multi-layer security by integrating compression, chaos-based key sensitivity, standardized encryption, and share-based protection. This combination improves resistance to statistical, differential, and brute-force attacks while maintaining acceptable computational complexity and bandwidth efficiency, making the proposed scheme suitable for secure image transmission over public and untrusted networks.

4. Mathematical Formulation of the Proposed Scheme

A. Chaotic Map for Key Generation

A one-dimensional chaotic map is employed to generate highly sensitive pseudo-random sequences for key generation and permutation control. The logistic map is selected due to its simplicity and strong chaotic behaviour, and is defined as

$$x_{n+1} = \mu x_n (1 - x_n) \qquad (1)$$

Where $0 < x_0 < 1$, $3.5699 < \mu \leq 4$

The generated chaotic sequence is

$$X = \{x1, x2, x_{MN}\}$$

The chaotic sequence {xn} is converted into an integer sequence suitable for cryptographic operations using

$$k_i = \lfloor x_i \times 1014 \rfloor \bmod (MN) \qquad (2)$$

The image is reshaped into a 1-D vector:

$$I_v = [i1, i2, \ldots, i_{MN}]$$

A permutation operator π is applied:

$$I_p = \pi(I_v, k) \qquad (3)$$

Where Ip denotes the **chaotically permuted image vector**.

B. AES Key Integration

The permuted image is divided into 128-bit blocks:

$$B_j=\{b_{j,1},b_{j,2},\ldots,b_{j,128}\}$$

AES encryption is performed using a secret key KAES

$$C_j=AES_{Enc}(B_j,K_{AES}) \quad (4)$$

The overall AES-encrypted image is given by:

$$C=\bigcup_{j=1}^{L} C_j \quad (5)$$

Where L=(MN×8)/128

C. Burrows–Wheeler Compression Model

Let SSS be the serialized pixel sequence of the input image. The Burrows–Wheeler Transform rearranges SSS into a new sequence SBWTS_ {BWT} SBWTas

SBWT=BWT(S)(6)S_{BWT} = \text{BWT}(S) \SBWT=BWT(S) (6)

The inverse transformation reconstructs the original sequence using

S=BWT−1(SBWT) (7)

This process ensures lossless compression, preserving image fidelity after decryption.

D. Visual Cryptography Share Generation

The encrypted image CCC is divided into nn shares using a (k,n)(k,n)(k,n) visual cryptography scheme:

{S1, S2,…,Sn}=VC(C) (8)

Reconstruction is possible only when at least kkk valid shares are combined:

C=VC−1(S1, S2,⋯,Sk) (9)

Individual shares do not reveal any perceptual information about CCC.

E. Key Space Analysis

The total key space K of the proposed scheme is defined a

K=2128×1014×1014 (10)

where:

- 2128 corresponds to the AES key space,
- 1014 corresponds to the precision of x0x_0x0,
- 1014 corresponds to the precision of μ\muμ.

Thus,

K≈2128×1028 which is sufficiently large to resist brute−force attacks.

F. Security Implication

Due to the extreme sensitivity of the chaotic parameters x0x_0x0 and μ\muμ, even a variation of 10−14 results in a completely different encrypted output. This ensures strong resistance against brute-force, statistical, and differential attacks

4. 1 Statistical and Differential Security Metrics

A. Number of Pixels Change Rate (NPCR)

The Number of Pixels Change Rate (NPCR) measures the percentage of pixel differences between two encrypted images obtained from two plaintext images that differ by only one pixel. It evaluates the resistance of the encryption scheme to differential attacks.

Let C1C_1C1 and C2C_2C2 denote two cipher images of size M×NM. NPCR is defined as

$$NPCR= 1M×N \sum i= 1M \sum j= 1ND(i,j)×100\% \quad (11)$$

where

$$D(i,j)=\{0,C1(i,j)=C2(i,j)1,C1(i,j)≠C2(i,j) \quad (12)$$

A higher NPCR value indicates strong sensitivity to minor plaintext changes.

B. Unified Average Changing Intensity (UACI)

The Unified Average Changing Intensity (UACI) quantifies the average intensity difference between two encrypted images, further measuring diffusion effectiveness.

UACI is defined as

$$UACI= 1M×N \sum i= 1M \sum j= 1N | C1(i,j)−C2(i,j) | 255×100\% \quad (13)$$

Higher UACI values reflect stronger diffusion properties and improved resistance to differential cryptanalysis.

C. Information Entropy

Information entropy evaluates the randomness of the encrypted image. For an ideal 8-bit grayscale image, the entropy value approaches 8.

The entropy HHH of an encrypted image is computed as

$$H=−\sum i=0255 p(i) log2 p(i) \quad (14)$$

Where p(i) denotes the probability of occurrence of the gray-level value.

An entropy value close to 8 indicates that the encrypted image exhibits near-uniform gray-level distribution, making statistical attacks ineffective.

D. Security Interpretation

In a secure image encryption scheme, NPCR values close to 99.6% UACI values near 33% and entropy values approaching 8 demonstrate strong resistance against statistical and differential attacks. The proposed hybrid scheme achieves values close to these ideal benchmarks, confirming its robustness.

5. Result Analysis and Discussion

The performance of the proposed **Hybrid Chaos–AES Image Encryption Scheme** was evaluated in terms of **encryption/decryption time, computational complexity, and efficiency**. The results are compared with **AES-only** and **Chaos-only** encryption methods to highlight the benefits of the hybrid approach.

Fig. 2. a) Original Images b) Compressed Images c) Encrypted Images (AES) d} Encrypted Images (Choas) e) Encrypted Images (VC) f) Decrypted Images g) Decompressed Images h) Original Images.

.

5.1. Encryption and Decryption Time

Table 1: Encryption and Decryption Time

Test Images	Encryption Time (sec)			Decryption Time (sec)		
	AES	DES	Hybrid	AES	DES	Hybrid
LAKE	2.49	1.51	3.45	1.72	1.86	2.8
VEGETABLES	4.15	3.77	5.5	2.64	1.4	3.2
CAR	4.26	2.89	5.5	3.63	1.13	4.2
BABOON	4.4	3.18	5	2.01	0.78	3.1
FLIGHT	5.27	2.13	6.2	1.62	0.28	2.3

The hybrid scheme incurs a slight increase in computational time compared to AES and DES. Due to the additional chaotic pre-processing and Visual cryptography.

Table 2: Comparative Performance and Security Metrics

Method	NPCR (%)	UACI (%)	Entropy
AES-Only	95.01	30.95	6.987
Chaos-Only	96.05	31.00	6.991
Hybrid Chaos–AES	99.63	33.12	7.998

The hybrid scheme achieves **higher NPCR, UACI, and entropy**, confirming enhanced security. Computational overhead is minimal compared to the security gain.

6. .Conclusion

This work presents a novel hybrid image encryption scheme that combines chaos-based pixel permutation and diffusion with AES block encryption. The proposed approach addresses the limitations of traditional encryption methods when applied to digital images, including vulnerability to statistical attacks and inefficiency in handling image redundancy .Key contributions and findings are that Enhanced Security were achieved in Chaos-based permutation and diffusion disrupt pixel correlations and increase sensitivity to plaintext changes .AES provides standardized cryptographic strength, making the scheme resistant to brute-force, differential, and statistical attacks. Robustness and Randomness are achieved by Experimental results demonstrate high NPCR (>99%) and UACI (~33%) values. Efficiency and Practicality is proved by Encryption and decryption times are reasonable, even for high-resolution images, making the scheme suitable for real-time applications.

6.1 Future Work:

Extending the scheme to real-time video encryption. Exploring dynamic chaotic maps to further enhance key space and unpredictability. Investigating hardware implementations (FPGA/GPU) to improve encryption speed for large datasets. Incorporating adaptive AES modes (CBC, CTR) for additional security against specific attack models.

REFERENCES

1. M. Kaur and V. Kumar, “A comprehensive review on image encryption techniques,” Archives of Computational Methods in Engineering, vol. 27, no. 1, pp. 15–43, 2020.
2. Gonzalo Alvarez and Shujun Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129–2151, 2006.
3. X. Wu, K. Wang, and J. Kurths, “Color image encryption based on DNA encoding and spatiotemporal chaotic systems,” Information Sciences, vol. 349–350, pp. 273–287, 2016.

4. H. Liu, X. Wang, and A. Kadry, “Image encryption using chaotic map with symmetric diffusion structure,” Optics & Laser Technology, vol. 84, pp. 1–12, 2016.
5. R. Nahta, T. Jain, A. Narwaria, H. Kumar, and R. K. Gupta, “Image encryption–decryption using simple and modified version of AES,” in Smart Systems and IoT: Innovations in Computing, Singapore: Springer, 2020, pp. 641–653.
6. M. Ben Farah, A. Farah, and T. Farah, “An image encryption scheme based on a new hybrid chaotic map and optimized substitution box,” Nonlinear Dynamics, vol. 99, no. 4, pp. 3041–3064, 2020.
7. Moni Naor and Adi Shamir, “Visual cryptography,” in Advances in Cryptology—EUROCRYPT ’94, Lecture Notes in Computer Science, vol. 950. Berlin, Germany: Springer, 1995, pp. 1–12.
8. C. Blundo, A. De Santis, and D. R. Stinson, “On the contrast in visual cryptography schemes,” Journal of Cryptology, vol. 12, no. 4, pp. 261–289, 1999.
9. K. H. Lee and P. L. Chiu, “An extended visual cryptography scheme for color images using random grids,” Pattern Recognition, vol. 40, no. 10, pp. 2820–2830, 2007.
10. Michael Burrows and David Wheeler, “A block-sorting lossless data compression algorithm,” Digital Equipment Corporation Technical Report, 1994.
11. Khalid Sayood, Introduction to Data Compression, 4th ed. Burlington, MA, USA: Morgan Kaufmann, 2012.
12. D. Salomon and G. Motta, Handbook of Data Compression. London, U.K.: Springer, 2010.
13. A. Jolfaei and A. Mirghadri, “An image encryption approach using chaos and compression,” Journal of Systems and Software, vol. 105, pp. 161–172, 2015.
14. Y. Zhang, D. Xiao, and W. Wen, “Joint image compression and encryption using chaotic systems,” Multimedia Tools and Applications, vol. 74, no. 15, pp. 5965–5981, 2015.
15. Jacob Ziv and Abraham Lempel, “A universal algorithm for sequential data compression,” IEEE Transactions on Information Theory, vol. 23, no. 3, pp. 337–343, May 1977.
16. Xiaoling Wang and Yong Zhang, “A novel chaotic block image encryption algorithm based on dynamic random growth technique,” Optics and Lasers in Engineering, vol. 66, pp. 10–18, 2015.
17. Xuehu Yan, Shun Zhang, and Yong Zhou, “A chaos-based image encryption scheme using a permutation–diffusion structure,” IEEE Access, vol. 7, pp. 123–135, 2019.
18. Chunhua Li, Shujun Li, and Guanrong Chen, “On the security of a class of image encryption schemes based on permutation–diffusion architecture,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 10, pp. 1860–1870, 2014.
19. Kwok-Wo Wong, “A combined chaotic cryptographic and hashing scheme for secure multimedia communication,” IEEE Transactions on Systems, Man, and Cybernetics, vol. 38, no. 2, pp. 339–348, 2008.
20. Xiangyu Zhang, Jian Zhang, and Wei Liu, “Efficient joint compression and encryption for secure image transmission,” IEEE Transactions on Multimedia, vol. 20, no. 2, pp. 340–352, 2018.