NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 10, ISSUE 11, November – 2024

A REVIEW OF DIGITAL IMAGE ENCRYPTION: SCAN-PATTERN METHODS, CRYPTOGRAPHY, COMPRESSION AND HARDWARE ACCELERATION

Dr. Navpreet Kaur
Pt. C.L.S. Government College, Karnal (Haryana)India

Abstract
The rapid growth of digital imaging, multimedia communication, medical information systems, remote sensing, surveillance and embedded vision has increased the need for reliable protection of image data. Unlike conventional textual data, digital images contain substantial redundancy and strong spatial relationships between neighboring pixels. These characteristics create both challenges and opportunities for cryptographic design. Consequently, numerous image-encryption techniques have been proposed using permutation, substitution, chaotic transformations, scan patterns, XOR operations, compression and hardware acceleration. This review critically examines three supplied studies representing complementary aspects of image security: a scan-pattern and XOR-based image-encryption method, a general study of cryptography, encryption and compression, and an FPGA-oriented approach to image processing and secure transmission. The hardware-oriented study demonstrates the feasibility of implementing image-processing operations and encrypted transmission on FPGA platforms, while the cryptography and compression study emphasizes confidentiality, authentication, integrity and efficient data representation. This review further considers contemporary authenticated-encryption approaches, including AES-GCM and ChaCha20-Poly1305, and discusses why statistical randomness alone cannot establish cryptographic security. The analysis identifies important research gaps involving authenticated encryption, key management, nonce handling, reproducibility, hardware security and resistance to realistic attack models.

Keywords: Digital image encryption; cryptography; scan patterns; XOR; permutation; diffusion; image security; compression; FPGA; authenticated encryption; NPCR; UACI.

1. Introduction

Digital images have become one of the most important forms of digital information. Images are continuously generated and exchanged through smartphones, medical equipment, satellites, surveillance systems, industrial inspection systems, cloud platforms and communication networks. The increasing use of images has consequently created significant requirements for confidentiality, integrity, authentication and secure storage.

Image information is different from ordinary textual information because it contains a large number of highly correlated data elements. In a natural image, neighboring pixels normally have similar intensity values. This spatial correlation makes ordinary data characteristics unsuitable for direct assessment of an image-encryption system. A successful encryption process should substantially reduce the relationship between neighboring pixels and prevent an observer from extracting meaningful information from statistical properties of the ciphertext.

The supplied literature identifies this spatial correlation as one of the central characteristics of image data. The scan-pattern study explains that neighboring pixels in natural images generally exhibit strong

relationships and proposes scan patterns to rearrange image elements before applying an XOR-based transformation.

The security problem becomes even more important when images are transmitted through an insecure communication channel. An attacker may attempt to intercept, modify, replay or analyze image information. Therefore, a secure image-transmission system must not only make the original image unintelligible to unauthorized observers but should ideally also detect unauthorized modification.

Cryptography provides the mathematical foundation for protecting digital information. The supplied review on cryptography, encryption and compression identifies confidentiality, authentication, integrity and non-repudiation among the major objectives of information security. Encryption transforms plaintext into ciphertext using a cryptographic key, whereas decryption reconstructs the original information when the appropriate secret information is available.

Image encryption has consequently developed as a specialized research area. Researchers have investigated permutation-based techniques, substitution techniques, chaotic systems, transform-domain methods, selective encryption, scan patterns and combinations of these approaches. The supplied scan-pattern paper is particularly relevant because it attempts to achieve rapid encryption by combining structured pixel rearrangement with the simple XOR operation. It reports a three-stage process involving block rearrangement, rearrangement within blocks and XOR transformation.

Another important dimension is implementation efficiency. High-resolution images contain millions of pixels, and real-time systems may need to process multiple frames per second. Software-only implementations may therefore face limitations related to latency, memory bandwidth and energy consumption. Field Programmable Gate Arrays (FPGAs) provide a programmable hardware platform capable of exploiting parallelism and pipelining. The supplied hardware-oriented study investigates image processing and secure communication using FPGA platforms and demonstrates encrypted image transmission between hardware systems.

The purpose of this review is therefore not simply to summarize individual studies. Instead, it critically examines how image characteristics, cryptographic techniques, compression and hardware implementation interact. It also considers the distinction between statistical evidence of an effective image cipher and the stronger requirements of modern cryptographic security.

2. Objectives:

The major objectives of this review are:

1. To examine the characteristics of digital images that influence encryption design.
2. To analyze scan-pattern and XOR-based image encryption.
3. To review cryptographic and compression principles relevant to image security.
4. To examine FPGA-based implementation of image processing and secure transmission.
5. To discuss commonly used image-encryption evaluation parameters.
6. To compare the strengths and limitations of different approaches.

3. Fundamental Concepts of Digital Image Encryption

Digital Images as Data:

A digital image can be represented as a two-dimensional matrix of pixels. In a grayscale image, each pixel commonly represents an intensity value, while a color image may contain separate red, green and blue channels. A large image can therefore contain millions of numerical values.

This structure creates considerable redundancy. Adjacent pixels frequently possess similar values because objects and surfaces normally change gradually across an image. While this property is useful for image compression and recognition, it creates a potential weakness if an encryption method does not sufficiently destroy the spatial relationships.

The scan-pattern literature specifically exploits this observation. By changing the positions of blocks and then changing the positions of pixels within the blocks, the algorithm attempts to reduce the relationship between neighboring image elements before applying its final XOR operation.

Plain Image and Cipher Image

The original readable image can be considered the plain image or plaintext. After encryption, it becomes a cipher image or ciphertext.

A secure cipher image should ideally reveal no useful visual information about the original image. It should also exhibit statistical properties that make the original image difficult to infer.

However, visual randomness should not be confused with complete cryptographic security. A cipher image may look completely random while the underlying encryption mechanism contains weaknesses in its key generation, key management, authentication or resistance to chosen-plaintext attacks.

Symmetric Encryption

Symmetric cryptography uses a shared secret key for encryption and decryption. This approach is particularly attractive for large image files because symmetric algorithms are generally much faster than public-key operations.

The supplied cryptography review distinguishes symmetric and asymmetric encryption and describes the use of a common secret key in symmetric systems.

The scan-pattern algorithm reviewed in this paper is also symmetric and uses the same 128-bit key for encryption and decryption.

Asymmetric Cryptography

Asymmetric cryptography uses mathematically related public and private keys. It is generally more computationally expensive than symmetric encryption and is therefore not normally the preferred mechanism for encrypting every pixel of a large image.

Instead, asymmetric mechanisms can be used for authentication, digital signatures or secure establishment of symmetric session keys. This separation allows a system to use the efficiency of symmetric cryptography while retaining the advantages of public-key techniques for key establishment.

4.Review of the Literature

Scan-Pattern and XOR-Based Image Encryption

The principal image-encryption paper proposes a fast algorithm based on predefined scan patterns and XOR. The central idea is to exploit the two-dimensional structure of images by changing the order in which blocks and pixels are arranged.

The algorithm consists of three main stages.

Stage 1: Block Rearrangement

The input image is divided into blocks and the blocks are rearranged according to a selected scan pattern. For the reported experiments, 512 × 512 images are divided into 8 × 8 blocks.

The objective is to destroy large-scale spatial relationships. Pixels that were previously close to one another may become separated in the transformed image.

Stage 2: Pixel Rearrangement

After block-level rearrangement, the pixels inside individual blocks are rearranged using scan patterns. This provides another level of permutation and further reduces local relationships.

Stage 3: XOR Transformation

The transformed image is divided into four parts, and XOR operations are applied using selected image blocks. The study reports a 128-bit key divided among the three stages:

- 48 bits for the first stage,
- 48 bits for the second stage,
- 32 bits for the third stage.

The resulting system is attractive from an implementation perspective because XOR operations are computationally simple.

5. Security Analysis of the Scan-Pattern Method

Histogram Analysis

An image histogram describes the frequency distribution of intensity values. A natural image usually has a characteristic, nonuniform histogram. If an encrypted image retains a similar distribution, an attacker may potentially obtain information about the original image.

The supplied scan-pattern study reports that the cipher images have approximately uniform histograms, indicating that the encryption process substantially changes the intensity distribution.

Histogram analysis is therefore useful as a first-level statistical test.

However, histogram uniformity alone cannot establish cryptographic security. Two different images may have similar histograms, and a weak encryption algorithm can potentially produce a uniform histogram while still leaking information through other properties.

Correlation of Adjacent Pixels

Correlation analysis is especially important for image encryption because neighboring pixels in ordinary images are strongly related.

Correlation can be calculated in horizontal, vertical and diagonal directions. A strong encryption method should reduce these relationships.
The supplied study evaluates horizontal, vertical and diagonal correlations and reports cipher-image correlation values close to zero in many cases.
This indicates that the scan-pattern and XOR process successfully disrupts much of the original spatial structure.
Nevertheless, correlation should be interpreted as a diagnostic rather than a security proof.

Information Entropy

Information entropy measures uncertainty in a probability distribution. For an idealized uniformly distributed 8-bit grayscale image, the theoretical maximum Shannon entropy is 8 bits per pixel.
A cipher image approaching this value suggests that the distribution of intensity values is relatively uniform.
The supplied literature uses entropy as one component of security analysis.
Entropy is useful because low entropy may reveal nonuniformity. However, high entropy alone cannot demonstrate resistance against cryptanalysis. An attacker does not necessarily need to predict individual pixel values if weaknesses exist elsewhere in the encryption system.

Number of Pixels Change Rate

NPCR measures the proportion of pixels that change between two cipher images when a small change is introduced into the corresponding plain images.
The purpose is to evaluate diffusion. Ideally, changing one pixel in the input should cause changes throughout the encrypted output rather than remaining localized.
The supplied scan-pattern paper evaluates NPCR using a one-pixel change and reports high values across its test images.

Unified Average Changing Intensity

UACI measures the average difference in intensity between corresponding pixels in two ciphertext images generated from slightly different plaintext images.
Together, NPCR and UACI provide information about the sensitivity of an encryption system to small input changes.
The supplied study uses both measures as part of its differential-attack analysis.
However, modern evaluation should not rely exclusively on NPCR and UACI. These metrics are useful for image-specific statistical analysis but do not replace formal or empirical cryptanalysis.

6. Cryptography and Compression for Image Security

The second supplied study discusses cryptography, encryption and compression from a broader information-security perspective.
Cryptography protects information by transforming it into a form that unauthorized users should not be able to interpret. Compression, in contrast, reduces the amount of data required for storage or transmission. These two processes therefore address different problems.

Confidentiality

Confidentiality ensures that unauthorized users cannot obtain meaningful information from protected data.

For images, confidentiality is important in medical imaging, biometric applications, surveillance, personal photography, satellite imaging and proprietary industrial data.

Integrity

Integrity ensures that information has not been modified without authorization.

This requirement is particularly important for medical and scientific images. Even if an unauthorized modification is visually subtle, it may affect interpretation.

Authentication

Authentication establishes confidence about the source or identity associated with the data.

For image transmission, authentication can help determine whether the received image originated from the expected device or system.

Compression

The supplied literature emphasizes that compression can reduce storage requirements and communication costs.

Image compression may be either lossless or lossy.

Lossless compression allows exact reconstruction of the original image and is particularly appropriate for medical, scientific and archival applications.

Lossy compression reduces file size more aggressively but introduces irreversible changes. It may therefore be appropriate for consumer multimedia but not for every security-sensitive application.

7. Relationship Between Compression and Encryption

Compression and encryption should not be viewed as interchangeable technologies.

Compression attempts to remove redundancy, whereas secure encryption intentionally produces data that should appear highly unpredictable.

Consequently, compression is generally more effective before encryption. If secure ciphertext is highly random, conventional compression algorithms will normally have little exploitable redundancy.

A typical secure image-transmission pipeline can therefore be represented as:

Image acquisition → preprocessing → compression → encryption/authentication → transmission → decryption/authentication verification → decompression → reconstruction

The precise arrangement depends on the application.

For example, a medical imaging system requiring exact reconstruction should normally use lossless compression. A consumer image service may tolerate controlled lossy compression.

An important research opportunity is the development of compression-aware encryption systems that minimize bandwidth without weakening cryptographic protection.

8. FPGA-Based Image Processing and Secure Transmission

The third supplied study approaches image security from a hardware perspective.
The study emphasizes the growing importance of embedded image and video processing and describes FPGA technology as an attractive platform because it combines reprogrammability with hardware-level parallel processing.
The paper describes image processing operations including preprocessing, segmentation, feature extraction and recognition.

FPGA Architecture

The reported secure-transmission system uses two FPGA platforms:

- one FPGA performs encryption,
- another performs decryption,
- communication occurs through a transmission interface.

The paper describes a Xilinx Spartan 3E and Virtex 5 implementation and uses RC4 for the reported encrypted transmission experiment.
The study also integrates a display interface for observing the original, encrypted and decrypted images.

Hardware Image Processing

The FPGA architecture includes image-filtering and thresholding components. The supplied paper describes buffer lines, shift-register structures and parallel multiply-accumulate engines for image filtering.
For color images, the RGB channels are separated and processed individually before reconstruction.
This demonstrates the suitability of FPGA systems for image operations that contain significant parallelism.

Advantages of FPGA Implementation

FPGA-based image encryption and processing can offer several advantages:

1. Parallel processing.
2. Low processing latency.
3. Pipeline-based operation.
4. Reconfigurability.
5. Integration of image processing and communication functions.
6. Potentially high throughput.
7. Possibility of dedicated cryptographic hardware.

However, these advantages must be balanced against hardware resource utilization, power consumption, memory bandwidth and development complexity.

9. Critical Assessment of the Reviewed Approaches

The three supplied studies address different levels of the image-security problem.

Aspect	Scan-pattern/XOR method	Cryptography and compression	FPGA-based approach
Main objective	Image encryption	General information security	Secure image processing/transmission
Main technique	Permutation + XOR	Encryption + compression concepts	FPGA processing + encryption
Main advantage	Simplicity and image awareness	Broad security framework	Hardware acceleration
Major evaluation	Histogram, correlation, entropy, NPCR, UACI	Conceptual security properties	Hardware implementation
Key challenge	Cryptographic strength	General rather than image-specific evaluation	Hardware resources and security
Modernization needs	Stronger cryptographic foundation	Application-specific implementation	Replace legacy cryptography

The scan-pattern approach is valuable because it recognizes the unique structure of images. The use of scan patterns provides an intuitive mechanism for reducing spatial relationships. The reported statistical analysis also demonstrates that the method produces substantially altered cipher-image characteristics.

Nevertheless, a critical limitation is that statistical performance does not establish complete cryptographic security.

Similarly, the FPGA work demonstrates an important implementation concept but uses RC4 in its reported secure-transmission experiment.

Therefore, its architecture remains useful as a hardware/software co-design example, but the cryptographic component should be modernized for contemporary deployment.

16. Conclusion

Digital image security is a multidisciplinary problem involving image processing, cryptography, compression, communication and hardware implementation. The literature reviewed in this paper demonstrates that image-specific characteristics such as spatial correlation and redundancy strongly influence encryption design.

The scan-pattern and XOR approach reviewed here provides an interesting example of an image-aware encryption strategy. It performs block-level and pixel-level rearrangement followed by XOR transformation and evaluates its performance using histogram analysis, adjacent-pixel correlation, entropy, NPCR and UACI. The results reported by the original study indicate that the method can substantially reduce visible statistical relationships in the encrypted images.

The cryptography and compression literature demonstrates that confidentiality is only one component of information security. Authentication, integrity and efficient data representation are also important.

The FPGA-oriented work demonstrates the practical value of hardware acceleration for image processing and secure communication. Its use of multiple FPGA platforms illustrates how encryption can be incorporated into an embedded image-processing architecture.

However, the critical analysis shows that traditional image-encryption evaluation should not be confused with complete cryptographic validation. High entropy, low correlation, strong NPCR and favorable UACI values provide useful evidence about statistical behavior, but they cannot by themselves establish resistance to modern cryptanalytic attacks.

Modern secure systems should therefore move toward layered architectures. Image-specific processing can be used for efficiency, compression can reduce communication overhead, and standardized authenticated-encryption algorithms can provide the fundamental confidentiality and integrity guarantees. AES-GCM is specifically defined as an authenticated-encryption mode, while ChaCha20-Poly1305 provides another AEAD construction.

The future of secure image transmission is therefore likely to depend on integration rather than on a single encryption technique. Combining image-aware processing, appropriate compression, authenticated encryption, secure key management and FPGA/software co-design can provide a more complete and defensible approach to protecting digital visual information.

References

1. R. Moradi Rad, A. Attar and R. Ebrahimi Atani, “A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR,” International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 6, no. 5, pp. 275–290, 2013.
2. S. Kumari, “A Research Paper on Cryptography Encryption and Compression Techniques,” International Journal of Engineering and Computer Science, vol. 6, no. 4, pp. 20915–20919, 2017, doi: 10.18535/ijecs/v6i4.20.
3. S. Saha, C. Pal, R. Paul, S. Maity and S. Sau, “A Brief Experience on Journey through Hardware Developments for Image Processing and Its Applications on Cryptography,” supplied manuscript, University of Calcutta.
4. S. S. Maniccam and N. G. Bourbakis, “Image and Video Encryption Using SCAN Patterns,” Pattern Recognition, vol. 37, no. 4, pp. 725–737, 2004.
5. S. S. Maniccam and N. G. Bourbakis, “Lossless Image Compression and Encryption Using SCAN,” Pattern Recognition, vol. 34, no. 6, pp. 1229–1245, 2001.
6. M. Dworkin, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC,” NIST Special Publication 800-38D, National Institute of Standards and Technology, 2007.
7. National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, 2023.
8. Y. Nir and A. Langley, “ChaCha20 and Poly1305 for IETF Protocols,” RFC 8439, Internet Research Task Force, 2018.
9. A. Popov, “Prohibiting RC4 Cipher Suites,” RFC 7465, Internet Engineering Task Force, 2015.
10. M. A. E. Wahed, S. Mesbah and A. Shoukry, “Efficiency and Security of Some Image Encryption Algorithms,” Proceedings of the World Congress on Engineering, 2008.
11. J. C. Yen and J. I. Guo, “A New Chaotic Key-Based Design for Image Encryption and Decryption,” IEEE International Conference on Circuits and Systems, 2000.

12. A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna, "A New Image Encryption Approach Using Combinational Permutation Techniques," Journal of Computer Science, vol. 1, no. 1, pp. 127–131, 2006.
13. A. Sinha and K. Singh, "A Technique for Image Encryption Using Digital Signature," Optics Communications, vol. 218, no. 4, pp. 229–234, 2003.
14. M. V. Droogenbroech and R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images," Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002.