TUNIS BUSINESS SCHOOL
UNIVERSITY OF TUNIS

IT 360
INFORMATION ASSURA NCE & SECURITY

Security Project
Image Encryption

Authors:
Majd Hamdi
Seif Ben Soltana

Submitted to:
Prof. Manel Abdelkader

I/ Tools:

1- Online Websites for Encryption:

Characteristics:

- Operate through a web browser without the need to install software.
- User-friendly interfaces.
- Quick and easy for occasional or one-time use.

Advantages:

- Convenience: Accessible from anywhere with an internet connection.
- Ease of Use: Typically designed for users without technical background.
- Immediate: No setup or installation required.

Limits:

- Privacy Concerns: Uploading sensitive images to a third-party server poses inherent privacy risks.
- Limited Encryption Options: May offer fewer customization options for encryption methods and strength.
- Dependence on Internet: Requires a stable internet connection.

2- Coding based Softwares:

Characteristics:

- Utilize programming libraries (e.g. OpenCV in Python) to encrypt images.
- Offer extensive customization and automation capabilities.

Examples:

- Java with Bouncy Castle API: A comprehensive cryptography API that supports a wide range of encryption algorithms and techniques.

- Ruby with the OpenSSL Wrapper: Ruby's OpenSSL wrapper provides encryption capabilities, leveraging the existing OpenSSL library.

Advantages:

- Flexibility: Highly customizable encryption methods and parameters.
- Automation: Ability to script processes for encrypting multiple images or integrating encryption into larger workflows.
- Control Over Privacy: Images never leave your local environment unless you choose to share them.

Limits:

- Requires Programming Knowledge: Not suitable for users without coding skills.
- Setup Time: Requires initial setup and potentially a learning curve to understand the encryption libraries.
- Resource Intensive: Depending on the algorithm and encryption process, it might be slower than using specialized software, especially for large batches of images.

3- GUI based Softwares:

Characteristics:

- Standalone applications with graphical user interfaces (GUIs).
- Designed for a wide range of users, from novices to experts.
- Often support drag-and-drop functionality and one-click encryption.

Advantages:

- User-Friendly: Intuitive interfaces make it easy to encrypt images without technical knowledge.
- No Programming Required: Ideal for users who prefer a straightforward, no-code approach.
- Versatile: Many such applications offer various encryption standards and strengths.

Limits:

- Software Installation: Requires downloading and installing software, which may not be feasible on all systems or environments.
- Privacy: While more secure than online solutions, there's still a level of trust required in the software provider.
- Potentially Limited Encryption Options: Some applications may not offer the same breadth of encryption algorithms and configurations as programmable solutions.

4- Hardware Encryption Devices:

Characteristics:

- Physical devices designed to encrypt data, including images, through hardware rather than software.
- Can be in the form of USB drives or external hard drives with built-in encryption capabilities.

Advantages:

- High Security: Often feature robust encryption algorithms implemented at the hardware level, making them less vulnerable to software-based attacks.
- Portability: Easy to carry and use across different systems without the need for software installation.
- Simplicity: Encryption can be as easy as copying files to a drive.

Limits:

- Cost: Typically more expensive than software solutions.
- Physical Security Risks: Being physical items, they can be lost or stolen, although the data remains encrypted.
- Capacity Limitations: Storage capacity might be less than that of standard drives, considering the cost.

II/ Algorithms:

1/ Traditional:

1- DES (Data Encryption Standard):

Characteristics:

- Symmetric key algorithm.
- Utilizes a 56-bit key, plus 8 bits for parity (total of 64 bits, but only 56 are effectively used for encryption).
- Operates on 64-bit blocks of data.
- Uses a combination of substitution and permutation techniques.

Advantages:

- Simplicity and ease of implementation.
- Was widely adopted and served as the basis for many encryption systems.

Limits:

- The 56-bit key size is relatively short by modern standards, making it susceptible to brute-force attacks; it can be cracked in a feasible amount of time with sufficient computing resources.
- Has been officially deprecated and is no longer considered secure for most applications.

2- AES (Advanced Encryption Standard):

Characteristics:

- Symmetric key algorithm.
- Supports key sizes of 128, 192, and 256 bits.
- Operates on 128-bit blocks of data, regardless of the key size.

- Uses a series of transformations including substitution, permutation, mixing, and key addition.

Advantages:

- Considered highly secure; no effective cryptanalytic attacks have been found against it as of my last update.
- Efficient in both software and hardware implementations across a wide range of platforms.
- The standard encryption method recommended by many security protocols and organizations.

Limits:

- While efficient, the computational workload is heavier compared to some simpler, less secure algorithms, especially on systems without specialized cryptographic hardware.
- Key management and exchange can be challenging in scenarios where a secure channel for key exchange isn't already established.

3- RSA (Rivest-Shamir-Adleman):

Characteristics:

- Asymmetric key algorithm.
- Uses a pair of keys: a public key for encryption and a private key for decryption.
- The security is based on the practical difficulty of factoring the product of two large prime numbers.
- Key sizes typically range from 1024 to 4096 bits for modern applications.

Advantages:

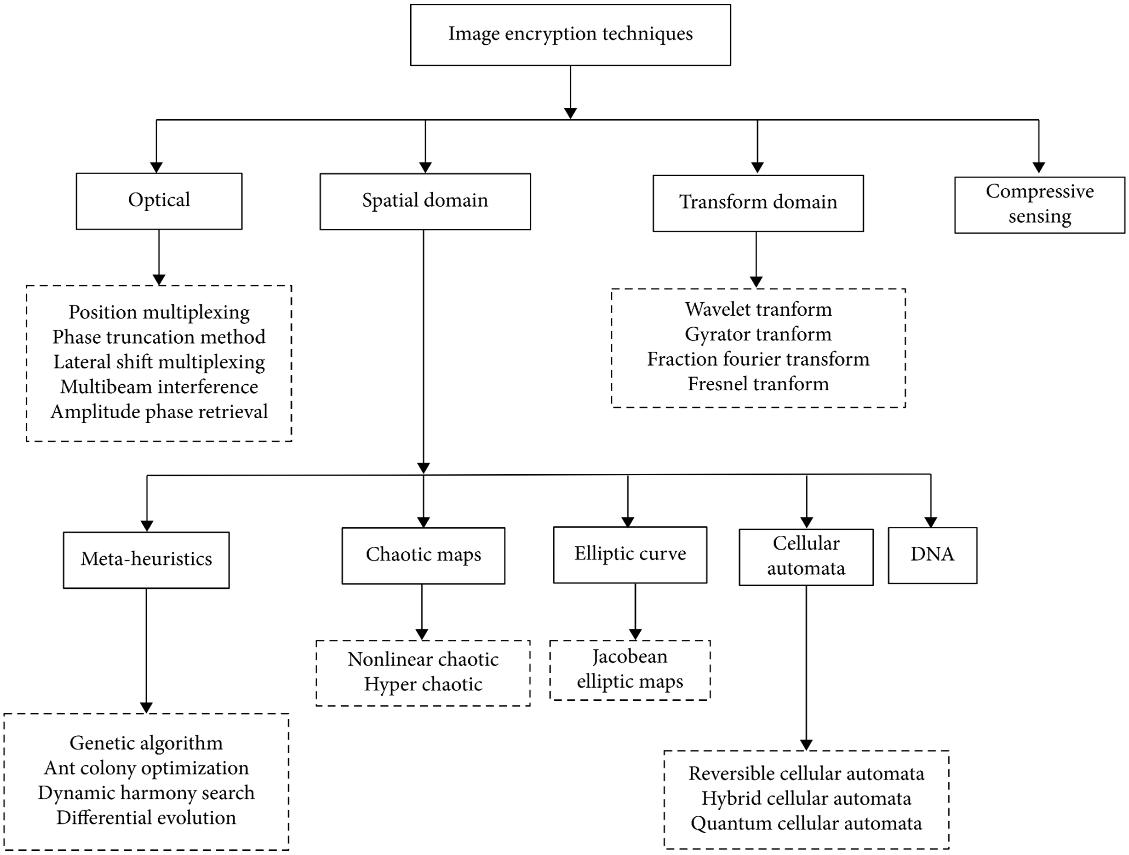
- Enables secure data transmission even if a secure channel isn't available for key exchange, solving a significant challenge faced by symmetric key algorithms.
- The public key infrastructure (PKI) supports digital signatures, making it useful for authentication and non-repudiation in addition to encryption.

Limits:

- Significantly slower than symmetric key algorithms like AES and DES, making it impractical for encrypting large amounts of data.
- Vulnerable to quantum attacks.
- Requires careful implementation and key management practices to maintain security.
- Security Evaluation: Because they are relatively new and less understood than traditional algorithms, evaluating the security of chaos-based methods can be difficult.
- Sensitivity to Implementation Details: The chaotic nature of these systems means that minor changes in implementation or computational inaccuracies can significantly impact performance and security.

2/ Modern:

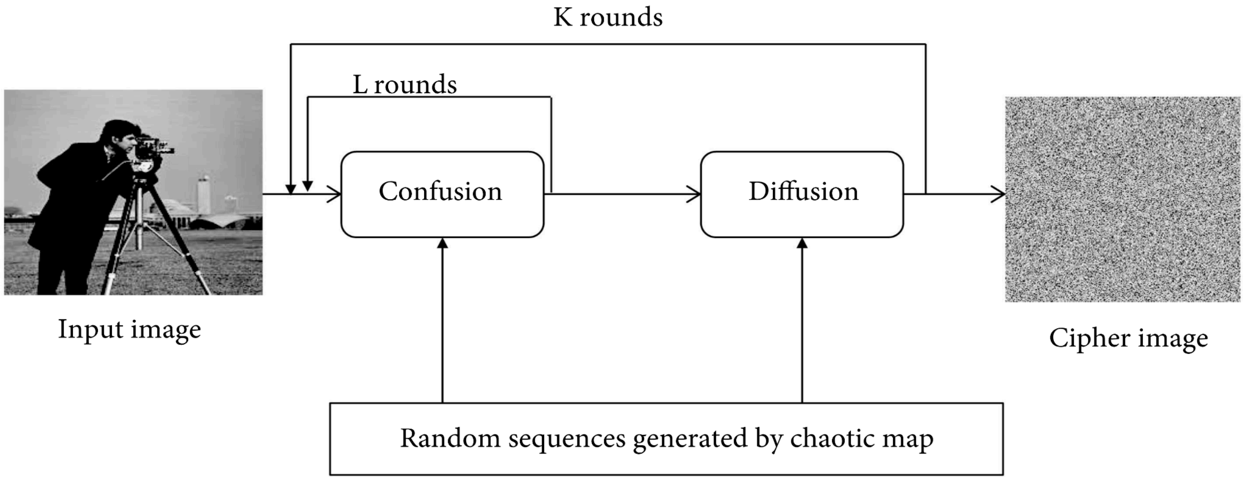
As traditional methods for image transmission and storage evolve, various image encryption techniques have emerged.



1- Image encryption in spatial domain:

The algorithms that are directly manipulating the pixels of the image are considered as spatial domain algorithms.

Examples of algorithms are:
A- Chaos-Based Image Encryption:
Characteristics:
Chaos-based encryption relies on unpredictable mathematical patterns (chaotic maps) to create secret keys. These maps exhibit dynamic behavior and are hard to crack. During encryption, they confuse and mix up the pixel values in the image.
Advantages:
Security: Chaotic maps generate unpredictable secret keys, enhancing security.
Dynamic Behavior: Chaotic behavior makes it challenging for attackers to decipher the encryption.
Efficient Operations: Confusion and diffusion operations are efficiently performed using chaotic maps.
Limits:
Key Management: Managing and securely distributing chaotic keys can be complex.
Sensitivity: Chaotic systems are sensitive to initial conditions, which may affect robustness.



Working of chaotic map-based image encryption.

B- Elliptic Curve-Based Image Encryption:

Characteristics:

Elliptic curve cryptography (ECC) offers memory-efficient encryption using mathematical curves. ECC requires smaller keys and is applied after converting color images to grayscale.

Advantages:

Security: Chaotic maps generate unpredictable secret keys, enhancing security.

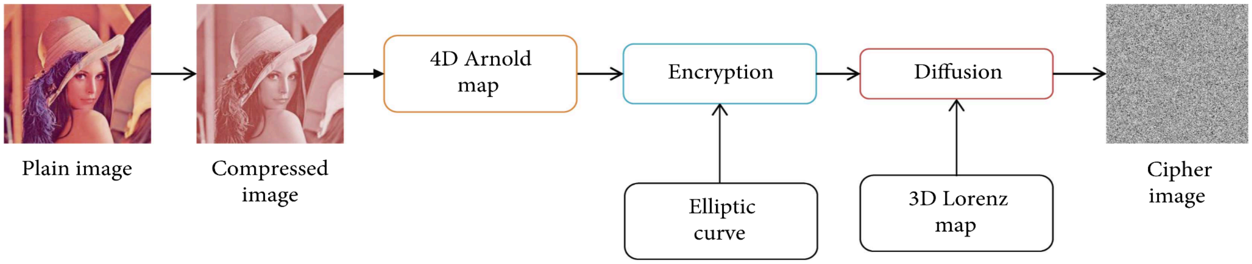
Dynamic Behavior: Chaotic behavior makes it challenging for attackers to decipher the encryption.

Efficient Operations: Confusion and diffusion operations are efficiently performed using chaotic maps.

Limits:

Key Management: Managing and securely distributing chaotic keys can be complex.

Sensitivity: Chaotic systems are sensitive to initial conditions, which may affect robustness.

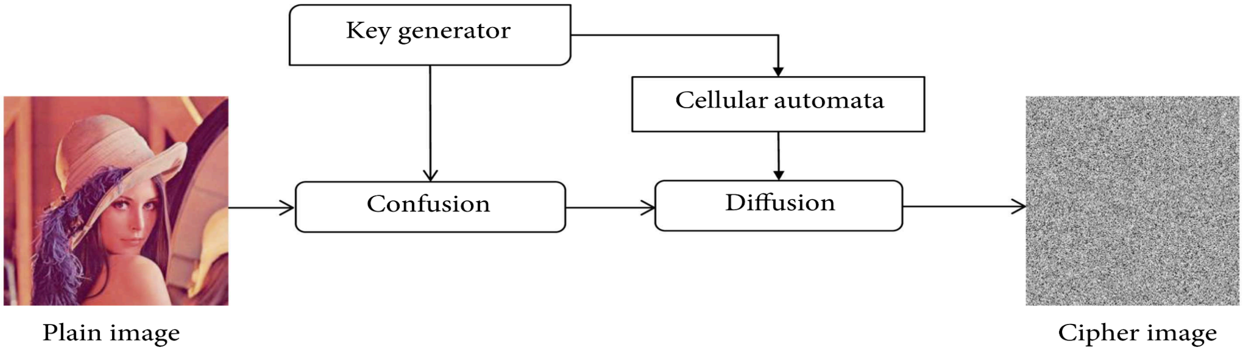


Chaotic map and elliptic curve-based image encryption.

C- Cellular Automata-Based Image Encryption:

Characteristics:

Cellular automata, like a game with complex rules, generate random sequences for encryption. Their simplicity and parallelism make them useful. In this approach, pixel values are diffused following specific rules.

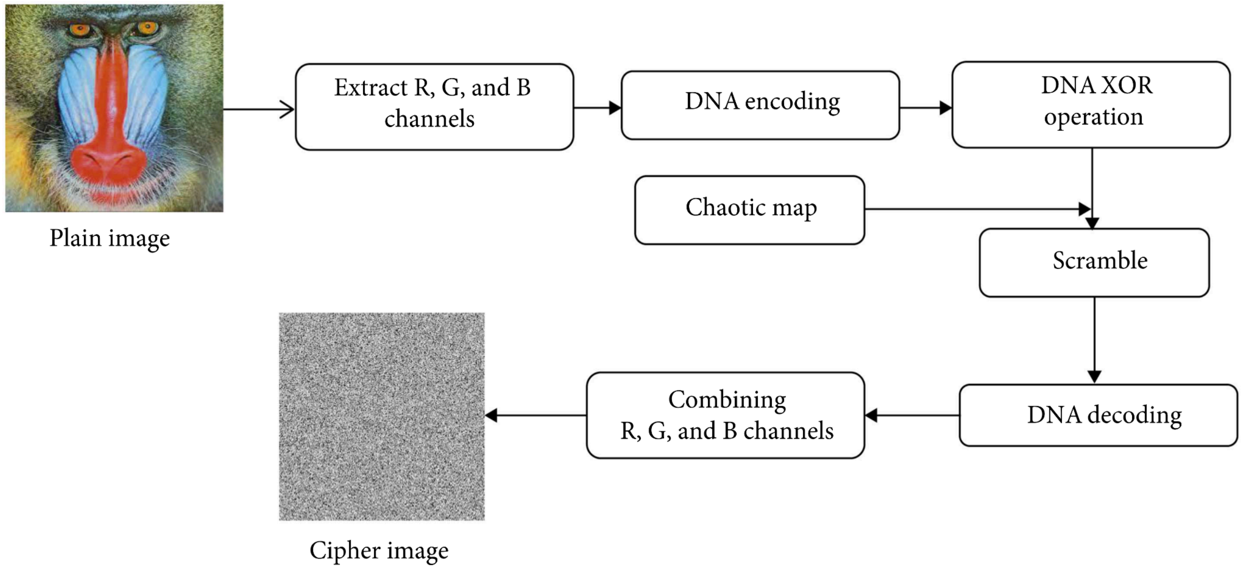


General framework of cellular automata-based image encryption.

Advantages:
Parallelism: Cellular automata generate random sequences in parallel.
Simple Hardware: Implementation is straightforward due to simple rules.
Robustness: Cellular automata models exhibit robust behavior.
Limitations:
Rule Selection: Choosing appropriate rules impacts security.
Limited Key Space: Cellular automata may have limited key diversity.

D- DNA-Based Image Encryption:

Characteristics:
Inspired by DNA properties, this method leverages massive parallelism, extensive storage, and ultra-low power consumption. Complementary DNA rules encode and decode image information. The process involves channel decomposition, XOR operations, and matrix scrambling.



DNA-based image encryption.

Advantages:
Massive Parallelism: DNA-based encryption leverages parallelism.
Ultra-Low Power: DNA properties allow energy-efficient encryption.
Storage Capacity: DNA can store large amounts of information.
Limits:
Biological Constraints: Practical implementation involves biological processes.
Encoding/Decoding Overhead: DNA encoding and decoding can be resource-intensive.

E- Metaheuristics-Based Image Encryption:

Characteristics:

Metaheuristics optimize encryption results. They explore multiple cipher images or fine-tune chaotic map parameters to enhance security. These algorithms aim to find the best encryption strategy.

Advantages:

Optimization: Metaheuristics find optimal encryption strategies.

Adaptability: Can adapt to different scenarios and data.

Efficient Key Tuning: Optimizes chaotic map parameters.

Limits:

Computational Cost: Metaheuristics may require significant computation.

Parameter Sensitivity: Proper tuning of metaheuristic par*a*meters is crucial.

2- Compressive Sensing-Based Image Encryption Characteristics:

Characteristics:

Compressive sensing combines compression and encryption in a single process. Imagine it as a two-in-one approach: first, it compresses the image using a special matrix; then, that same matrix becomes a secret key for encryption.

Advantages:

Dual Functionality: Compressive sensing performs compression and encryption simultaneously, saving computational resources.

Reduced Data Size: By compressing the image, it reduces storage and transmission requirements.

Key as Measurement Matrix: The same measurement matrix used for compression serves as a secret key for encryption.

Limits:

Complexity: Implementing both compression and encryption in a single step can be intricate.

Key Management: Ensuring secure distribution and management of the measurement matrix is essential.

3- Optical Image Encryption Algorithms

Characteristics:
Optical techniques are popular due to their speed and parallel processing capabilities. One such method is Double Random-Phase Encoding (DRPE). Here's how it works: the plain image is transformed into stationary white noise using two random phase masks. These masks act as keys for encryption.

Advantages:
Speed: Optical techniques offer fast encryption due to parallel processing.
Parallelism: Multiple operations can occur simultaneously, improving efficiency.
Robustness: Optical encryption methods are robust against noise and interference.

Limits:
Hardware Dependency: Requires specialized optical hardware for practical implementation.
Security Trade-offs: Some optical methods sacrifice security for speed.

4- Transform-Based Image Encryption Algorithms Characteristics:

Characteristics:
In transform-based encryption, the image transitions from its original spatial form to a frequency space using specific mathematical transforms. For color images, we break them down into three channels (red, green, and blue). Each channel undergoes permutation and diffusion processes. Finally, the inverse transform gives us the encrypted image.

Advantages:
Frequency Domain: Transform-based encryption shifts the image from spatial to frequency space, enhancing security.
Channel Independence: Color channels (R, G, B) can be independently processed, allowing flexibility.
Inverse Transform: The inverse transform recovers the original image during decryption.

Limits:
Processing Overhead: Transform operations can be computationally expensive.
Key Management: Proper management of keys and transform parameters is crucial.