ISSN: 2349-6193
Impact Factor: 3.866

IJESMR

International Journal of Engineering Sciences & Management Research

IMPROVE CRYPTOGRAPHY SCHEME FOR DATA TRANSFER

[1]Praveen Kumar and [2]Sanjay Kant
[1]Assistant Professor,[2]Assistant Professor
Department of Computer Application
Shri Ram College, Muzaffarnagar, Uttar Pradesh
[1]Email:-praveenkumarsrc2006@gmail.com
[1]Email:-sanjaykanttyagi@gmail.com

ABSTRACT

This paper a new method is presented for solving secure data transfer over network between two points with a boundary for parameter. As advancement in network technology, data security is an necessary part of the technology .the proposed scheme create visual cryptography achieves better and more convenient compare to existing method.

Key-words: Image encryption and decryption, ICS, cipher, Image Generator.

INTRODUCTION

ICS is a method for encrypted text, number in form of image and it is relatively new in the field of computer science by this cryptography scheme we transform data into cipher text and image this secure image pixel is strongly correlated value of matrix[1]. A new permutation and encryption scheme based on ICS[2]. The process of shifting and positions of data in the matrix before making image confuse the relationship of original data and cipher text[3].

METHODOLOGY

1. Analyze current scheme and identify weaknesses:

Identify the algorithm being used: Research the algorithm's security strength and known vulnerabilities.

Evaluate key management practices: Assess how keys are generated, stored, and distributed. Are there secure protocols in place?

Review data transfer protocols: Look for potential weaknesses in the protocol itself, like missing encryption or insecure communication channels.

Consider performance and efficiency: Encryption algorithms have varying processing demands and data size impacts.

2. Define security goals and requirements:

Data sensitivity: Determine the level of confidentiality, integrity, and authenticity required for the data.

Threat model: Identify potential attackers and their capabilities (e.g., casual eavesdroppers, targeted attackers with advanced resources).

Performance constraints: Consider limitations on processing power, memory, and bandwidth.

3. Research and explore improvement options:

ISSN: 2349-6193
Impact Factor: 3.866

IJESMR

International Journal of Engineering Sciences & Management Research

Explore newer, stronger algorithms: Research ongoing research in cryptography, particularly areas like post-quantum cryptography, and consider options that meet your security requirements.
Review key management best practices: Implement secure key generation, storage, and distribution practices that follow industry standards. Consider key rotation and secure key exchange protocols.
Investigate layered security approaches: Explore combining different cryptographic techniques like symmetric and asymmetric encryption or incorporating steganography for additional protection.
Review secure data transfer protocols: Research and adopt established protocols like HTTPS for secure communication over the internet.
4. Design, implement, and test the improved scheme:
Develop a plan for implementing the chosen improvements: This may involve integrating new libraries, modifying existing code, or updating infrastructure.
Thoroughly test the new scheme: Perform security testing to identify any vulnerabilities, and ensure performance meets your requirements.
Monitor and continuously improve: Stay updated on advancements in cryptography and threat landscape, and adapt your scheme as needed.
Additional considerations:
Seek expert advice: If dealing with highly sensitive data or complex security needs, consider consulting with cryptography experts.
Prioritize user experience: Balance robust security with user-friendliness. Complex key management can hinder adoption, so aim for a balance between security and ease of use.
Stay informed: Keep up-to-date with the latest advancements in cryptography and potential new threats to ensure your scheme remains effective.

PROPOSED METHOD

This is a new method for construction of image using data matrix
3.1: Encryption: Let s be the matrix
Original data:
S= {11000011, 11100011, 10010001, 10010010, 10010011, 10010100, 10010101, 10010110}

1	1	0	0	0	0	1	1
1	1	1	0	0	0	1	1
1	0	0	1	0	0	0	1
1	0	0	1	0	0	1	0
1	0	0	1	0	0	1	1
1	0	0	1	0	1	0	0
1	0	0	1	0	1	0	1
1	0	0	1	0	1	1	0

Transpose the data

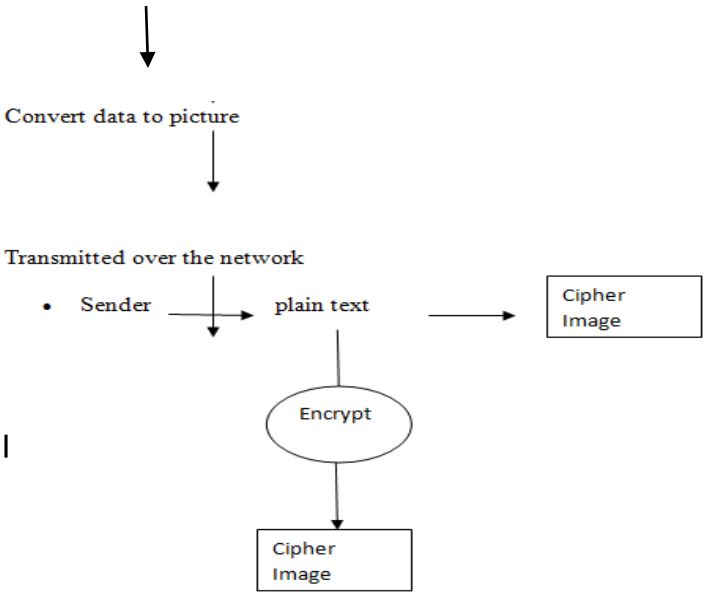
ISSN: 2349-6193
Impact Factor: 3.866

IJESMR

International Journal of Engineering Sciences & Management Research

1	1	1	1	1	1	1	1
1	1	0	0	0	0	0	0
0	1	0	0	0	0	0	0
0	0	1	1	1	1	1	1
0	0	0	0	0	0	0	0
0	0	0	0	0	1	1	1
1	1	0	1	1	0	0	1
1	1	1	0	1	0	1	0

- Add the private key
- Aij= {aij+a[0],aij+a[1],aij+a[2],aij+a[3],aij+a[4],aij+a[5],aij+a[6],aij+a[7],aij+a[8]}

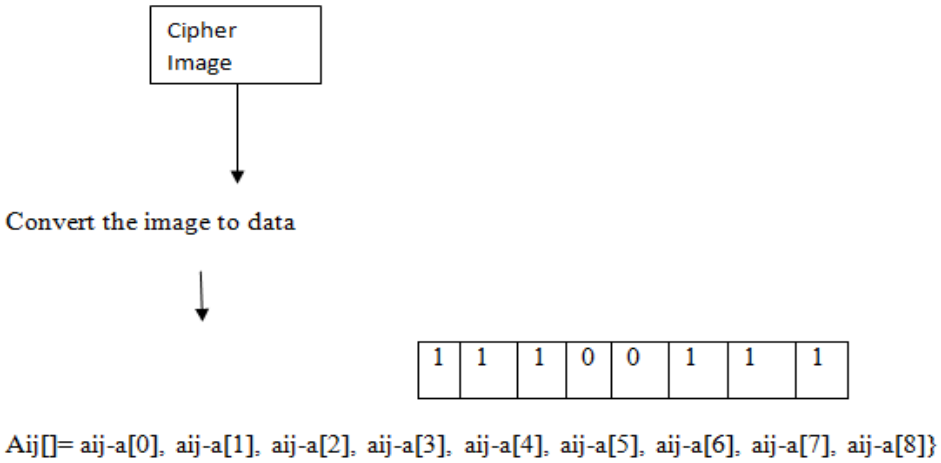


3.2 Decryption

ISSN: 2349-6193
Impact Factor: 3.866

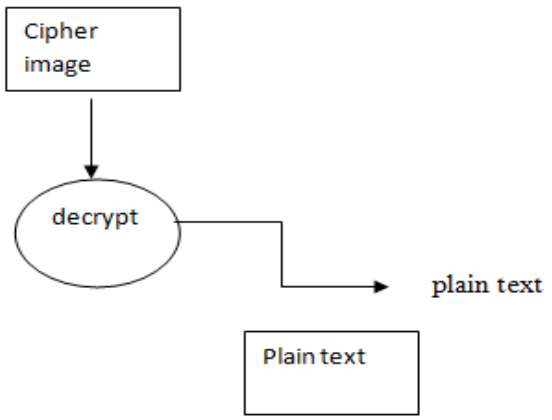
IJESMR

International Journal of Engineering Sciences & Management Research



Transpose the data

1	1	0	0	0	0	1	1
1	1	1	0	0	0	1	1
1	0	0	1	0	0	0	1
1	0	0	1	0	0	1	0
1	0	0	1	0	0	1	1
1	0	0	1	0	1	0	0
1	0	0	1	0	1	0	1
1	0	0	1	0	1	1	0



4. Image Generations:

The image generation can be done by Image Generator algorithms. this algorithm having specific meaning in each pixel

Step1: set the size(dimension) of image file

ISSN: 2349-6193
Impact Factor: 3.866

IJESMR

International Journal of Engineering Sciences & Management Research

Step2: create a object to hold the image
Step3: pick the value from matrix for red , green and blue color component
Step4: generated a Random number for RGB color set
Step5: Repeat the step3 and 4 until completion of image.

5. Module for image creation:

```
BufferImgImg;
Img=new BufferImg(width, height);
for(y=0; y<height; y++)
{
for(x=0 ; x<width; x++)
{
  red=(int)(random()*256)
 green=(int)(random()*256)
 blue=(int)(random()*256)
}
Img.setRGB(red, green , blue);
ImageIO.write(img)
```

6. Color Combination scheme:-

we use RGB color scheme for simplicity . variation of color has strongly correlation with different data.

RESULT & DISCUSSION

Using stronger algorithms: Cryptography relies on algorithms to scramble and unscramble data. Newer, more complex algorithms offer better protection against brute-force attacks trying every possible key combination. Research is ongoing in areas like post-quantum cryptography to stay ahead of potential threats from quantum computers.(https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers)

Key management: Even the strongest algorithm is useless if the key is compromised. Proper key management involves secure generation, storage, and distribution of keys. This may involve key rotation and secure key exchange protocols like Diffie-Hellman.

Layered security: Combining multiple security techniques can enhance overall protection. This could involve using a combination of symmetric and asymmetric encryption, or even incorporating steganography to hide the data within another file.

Protocol security: The way data is transferred can also be a vulnerability. Protocols like HTTPS (Hypertext Transfer Protocol Secure) encrypt communication between a web server and a browser, ensuring data privacy during web browsing.

CONCLUSION

In this paper we explain a method of cryptography in form of image the proposed method improve the security and easy to implement as compare to other similar method.

REFERENCES

1. Thomas Monoth& babu auto "an improved n out of n visual cryptography scheme" IJCSIT
2. A Generalization of the RSA Elatrash; Fayik Ramadan EL-Naowk –Journal of Applied science 1824-1826,2007 ISSN 1812-5654© 2007 Aian Network for Scientific information
3. Image Encryption Approach using self Invertible key Matrix of Hill Cipher Algorithm 1st International Conference on Advance in Computing ,Chikhli India 21-22 Feb 2008