Encryption Technique for Finger Biometric Image Using Rubik's Cube Principle and Arnold Transform

Pranoti G. Tapase[1], Prof. G. N. Wazurkar[2], Dr. D. R. Dandekar[3]
[1, 2] Dept of Electronics Engineering
[2]Assistant Professor, Dept of Electronics Engineering
[3]Professor, Dept of Electronics Engineering
[1, 2, 3] BDCE, Sevagram, Wardha –442102, INDIA

Abstract- *Now a days lot of people using multimedia, transferring data online and receiving also. Therefore, security of intimate data is become need. However, most of the networks used for multimedia distribution are open channels and are highly insecure. These networks are vulnerable to attacks and not suitable for transmitting sensitive and valuable multimedia content such as military, financial or personal videos. This necessitates secure encryption algorithms for multimedia data protection. Cryptography is an important tool in modern electronic security technologies to protect valuable multimedia data on intranets, extranets and the Internet.*

Keywords- Encryption algorithm, Rubik's Cube Principle, Arnold Transorm.

I. INTRODUCTION

The protection of images is of particular interest in this paper. Traditional image encryption algorithms such as private key encryption standards (DES and AES), public key standards such as Rivest Shamir Adleman (RSA), and the family of elliptic-curve-based encryption (ECC) ,as well as the international data encryption algorithm (IDEA),may not be the most desirable candidates for image encryption,especially for fast and real-time communication applications.In recent years, several encryption schemes have been proposed . These encryption schemes can be classified into different categories such as value transformation , pixels position permutation and chaotic systems .

In the past few years, several encryption algorithms based on chaotic systems have been proposed as means to protect digital images against cryptographic attacks. These encryption algorithms typically use relatively small key spaces and thus offer limited security,especially if they are one-dimensional. In this paper, we proposed a novel image encryption algorithm based on Rubik's cube and Arnold transform principle. The original image is scrambled using the principle of Rubik's cube. Then, XOR operator is applied to rows and columns of the scrambled image using two secret keys. Finally, the experimental results and security analysis show that the proposed image encryption scheme not only can achieve good encryption and perfect hiding ability but also can resist exhaustive attack, statistical attack, and differential attack

II. EXISTING SYSTEM

The existing technique is consist of single stage encryption using fuzzy commitment based scheme.

Another feature based encryption technique for securing forensic biometric image data using AES and visual cryptography.

Drawbacks of existing system:

- Encryption has the risk of information leakage for stored biometric template and is not suitable for online case.
- It has low entropy value 2.5 i.e very less.
- Single step encryption is not secure for real time transmission.

III. PROPOSED SYSTEM

a novel image encryption algorithm is proposed.

This algorithm is based on the principle of Rubik'scube and Arnold transform to permute image pixels. To confuse the relationship between original and encrypted images, the XOR operator is applied to odd rows and columns of image using a key. The same key is flipped and applied to even rows and columns of image. Experimental tests have been carried out with detailed numerical analysis which demonstrates the robustness of the proposed algorithm against several types of attacks such as statistical and differential attacks (visual testing). Moreover, performance assessment tests demonstrate that the proposed image encryption algorithm is highly secure.

Proposed methodology:

- Input fingerprint biometric image
- Preprocessing of input image
- Key generation
- Encryption /decryption algorithm
- Key management
- Performance evaluation using parameters under common attacks such as noise, geometric and compression.

Arnold Transform

It is applicable on square size image N X N and does not requires encryption and decryption key.

1. Encryption Process: (c',c'') & (xf,yf) are initial & final pixel coordinates. P = N.

$$\begin{bmatrix} xf \\ yf \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} c' \\ c'' \end{bmatrix} (mod\ p)$$

2. Decryption Process:

$$\begin{bmatrix} c' \\ c'' \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} xf \\ yf \end{bmatrix} (mod\ p)$$

Rubik's Cube Encryption algorithm-

Let I represent the 8-bit gray scale input biometric image of the size m x n. The steps involved in the encryption of the biometric image are as follows

1. Generate two vectors kr and kc of the length m and n respectively from the input biometric images randomly from any one row and column.
2. Decide the number of iterations imax and initialized counter i = 0.
3. For each row x in I
   a. Calculate the sum of all elements in the row x represented by ar(x)
   b. Compute modulo 2 of ar(x) represented by mar(x)
   c. Left or right circular shift each pixel elements kr(x) times according to following if mar(x) = 0 right shift else left shift.
4. For each column y in I
   a. Calculate the sum of all elements in the column y represented by ac(y)
   b. Compute modulo 2 of ac(y) represented by mac(y)
   c. Up or down circular shift each pixel elements kc(y) times according to following if mac(y) = 0 up shift else down shift.

Steps 3 and 4 will create a scrambled image represented by Is

5. Use vector kr to apply bitwise XOR operator on the each row of the partial resultant image Is using following equations

$$I\_1\ (x,y) = I\_s\ (m-x, n-y)\ XOR\ k\_r\ (x)$$

Where XOR is the XOR operator applied on flipped scrambled image upside down with vector kr(x).

6. Use vector kc to apply bitwise XOR operator on the each column of the partial resultant image I1 using following equations

$$I\_2\ (x,y) = I\_1\ (m-x, n-y)\ XOR\ k\_c\ (y)$$

Where XOR is the XOR operator applied on flipped partially encrypted image upside down with vector kc(y).

Rubik's Cube Decryption algorithm-

Let Ie represent the 8-bit gray scale input encrypted biometric image of the size m x n. The steps involved in the decryption of the encrypted biometric image are as follows

1. Obtain two vectors kr and kc of the length m and n respectively from the sender.
2. Decide the number of iterations imax and initialized counter i = 0.
3. Use vector kc to apply bitwise XOR operator on the each column of the encrypted image Ie using following equations

$$I\_11\ (x,y) = Ie\ (m-x, n-y)\ XOR\ kc\ (y)$$

4. Use vector kr to apply bitwise XOR operator on the each row of the partial resultant image I11 using following equations

$$I\_21\ (x,y) = I\_11\ (m-x, n-y)\ XOR\ kr\ (x)$$

5. For each column y in I21
   a. Calculate the sum of all elements in the column y represented by ac(y)
   b. Compute modulo 2 of ac(y) represented by mac(y)
   c. Up or down circular shift each pixel elements kc(y) times according to following if mac(y) = 1 up shift else down shift.
6. For each row x in I21
   a. Calculate the sum of all elements in the row x represented by ar(x)
   b. Compute modulo 2 of ar(x) represented by mar(x)

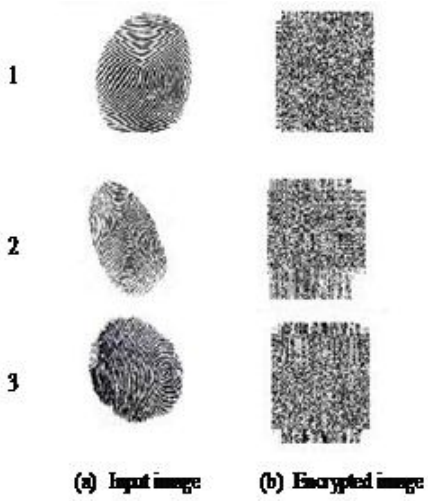
c. Left or right circular shift each pixel elements kr(x) times ac-cording to following if mar(x) = 1 right shift else left shift.

Steps 5 and 6 will create a final decrypted image represented by Id

7. Increment the counter i = i + 1.
8. Repeat steps 3 to 7 if i < imax else stop.

IV. RESULT AND DISCUSSION

Lossless encrypted template for finger biometric image as shown below –



This proposed technique is simple click and open application, it don't required any special setup, this proposed technique is also capable of fast encryption/decryption which is suitable for real-time Internet encryption and transmission applications..

V. CONCLUSION

Our proposed technique main objective is to avoid loss of encrypted template which happen due to external attacks like noise, geometric and compression hence this objective is achieved. So using this algorithm we can enhance the security of transmission, storage and verification.

VI. ACKNOWLEDGEMENT

I would like to thank respected Dr. D. R. Dandekar sir and Prof. G. N. Wazurkar sir for giving me such a wonderful opportunity to expand my knowledge and for his huge support. Secondly, I would like to thank my parents who patiently helped me as I went through my work.

REFERENCES

[1] Bin Liang, et al, "A Novel Fingerprint-Based Biometric Encryption," in IEEE Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2014.
[2] Quist-Aphetsi Kester, et al, "Feature Based Encryption Technique For Securing Forensic Biometric Image Data Using AES and Visual Cryptography," in IEEE Second International Conference on Artificial Intelligence, Modelling and Simulation, 2014.
[3] G. Bhatnagar and Q. J. Wu, "Enhancing the transmission security of biometric images using chaotic encryption," Springer Multimedia systems, vol. 20, no. 2, pp. 203–214, 2014.
[4] Brindha Murugan, Ammasai Gounden Nanjappa Gounder, "Image encryption scheme based on blockbased confusion and multiple levels of diffusion," in IET Computer Vision, Vol. 10 Issue 6, 2016, pp. 593-602.
[5] R. Gonzales, R. E. Woods, "Digital Image Processing," 2nd Edition, New Jersey Prentice Hall, 2002.
[6] A. K. Jain, "Fundamentals of Digital Image Processing," 2nd Edition, Prentice Hall, 1994.