JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURITY ANALYSIS FOR TRANSMISSION INFORMATION USED IN IMAGE AUTHENTICATION

Patarla lakshmi[1], Dr. M. Sailaja[2]

[1]Student, M.Tech (VLSI&ES), Department of Electronics and Communication Engineering UCEK(A), JNTU Kakinada, Andhra Pradesh, India,533003.

[2]Professor, Department of Electronics and Communication Engineering UCEK(A), JNTU Kakinada, Andhra Pradesh, India,533003.

- ***Abstract***– The requirement to ensure the safety of data sent between any two electronic systems has grown in tandem with the popularity of such transactions. The difficulty increases when trying to prevent unwanted access to sensitive user data. As a result, protecting sensitive user information using encryption is essential. The authenticity of the picture conveyed in the communication system relies on information about the sender, which is kept secret in this study. To protect the identity of the sender, their data is encrypted before being included in the message. Multiple encryption techniques may be used to encrypt the sender's data. In this work, we use the blowfish encryption method, a symmetric key block figure, to encode the information of the source of the image, which is put away as a text record of variable sizes. Blowfish employs a 64-bit key size for encryption and decryption, with the key length varying from 32 to 448 bits. The algorithm has a skeletal framework similar to a crystalline network. MATLAB is the tool used to complete the project.

Index terms: Encryption, decryption, encryption, blowfish, cipher block, embedding, authentication.

1. INTRODUCTION

- It is becoming more important to offer a secure video data transmission due to the rapid expansion of multimedia applications such as video surveillance, video conferencing, digital video broadcast, and distant learning. The military uses encrypted visual data for international communication. This collection of pictures has to be protected from falling into the wrong hands. The best method for protecting data sent in visual form is encryption. A standard encryption technique like Advance Encryption Standard (AES) is been implemented and compared with blowfish algorithm.

2.Cryptography

Cryptography is study for security of communication.

The field of cryptography may be split in two distinct ways:

1.Asymmetric key cryptography.

2.Symmetric key cryptography.

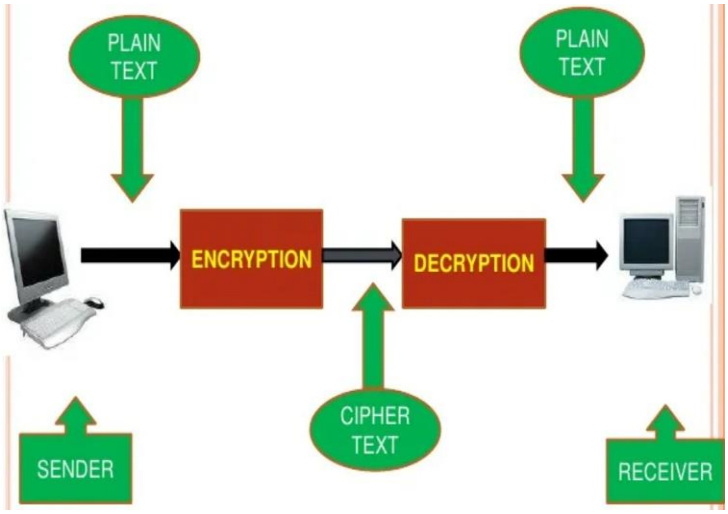


Figure 1: Encryption and decoding using cryptography

2.1 ASYMMETRIC KEY CRYPTOGRAPHY

- Step1: There are two distinct kinds of keys. Key Pair (Public and Private)
- Step2: The encryption and decryption processes rely on these keys.
- Step3: Using a public key, this method encrypts plaintext and transforms it into an unreadable code.
- Step4: Ciphertext into plaintext using private key and for decryption,

Example : Diffie-hell man, RSA, Digital Signature Algorithm and ECC

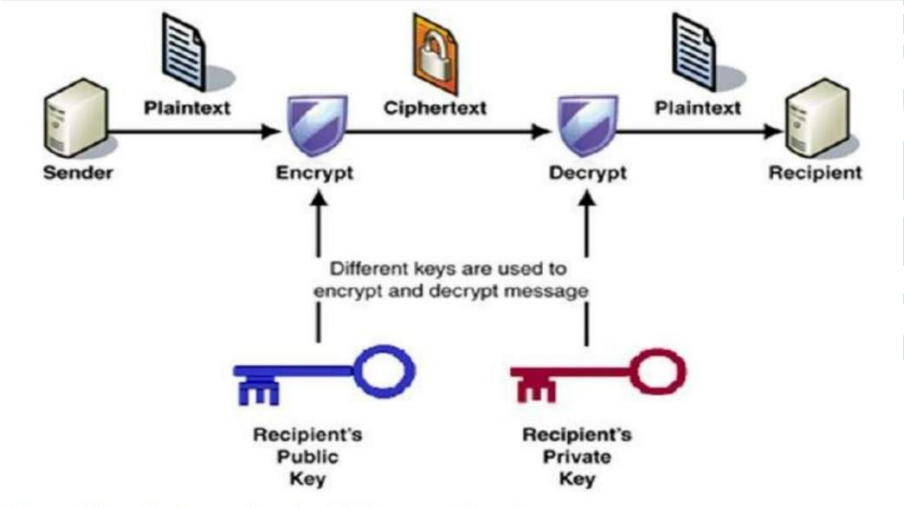


Figure 2: Asymmetric key cryptography for encryption and decryption

2.2 CRYPTOGRAPHY SYMMETRIC KEYS

Step1: By utilizing secret key both encryption and decoding is performed.

Step2: Utilizing a mystery key and encryption method, the source changes the plaintext into ciphertext and gives it to the beneficiary.

Step3: To convert encrypted text to plaintext, the same secret key is utilised as in the decryption process.

Example : Blowfish, DES, AES and 3DES

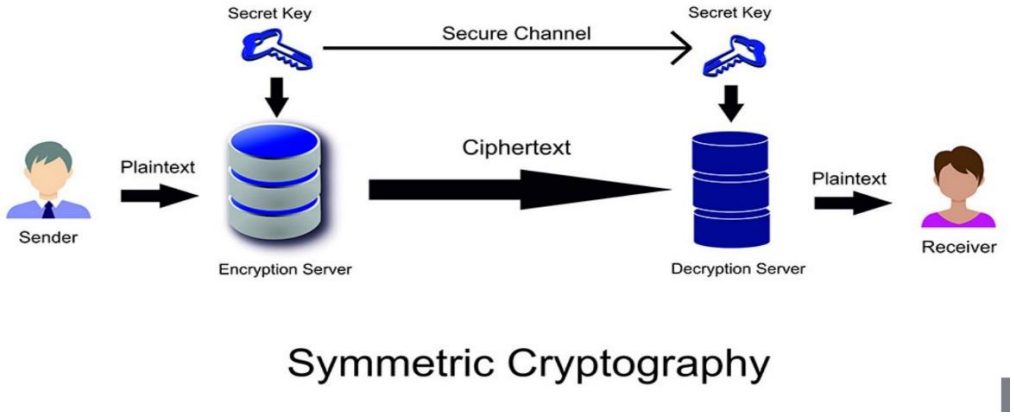


Figure 3: Symmetric key cryptography

2.3 FEATURE CLASSIFICATION

The cryptography uses encryption and decryption for security purpose using blowfish algorithm and AES (Advanced encryption standard),DES(Data encryption standard).etc,

2.3.1 Blowfish algorithm

Using a Feistel network, this symmetric block cypher encrypts data for a total of 16 cycles. P-array and S-boxes are the two arrays that make up this structure [9]. The P-array has eighteen 32-bit keys, labelled P1 through P18. Four Sboxes with 32-bit architecture are available. There are 256 digits in each S-box. Here's how we come up with the individual keys: The P-array and the four S-boxes are initialised by taking into account a proportion of the constant pi. To do this, we first XOR P1 with the initial 32 pieces of the key, and afterward we XOR P2 with the accompanying 32 pieces of the critical that come just after it.The process of XORing the bits of the key to generate a new P-array is repeated until the whole array has been processed.

Then, the 64-bit block of zeroes is encrypted using S blocks and a symmetric key public key array. • P1 and P2 are adjusted based on the data collected in Step 3. After step 3, the newly modified sub-keys are used to encrypt the output. • In order to adjust P3 and P4's output, we need Step 5. • All the items in the P-array and S boxes are updated by repeating the preceding stages. Indicative of the blowfish cypher and decryption technique. specifies information on a single blowfish. This disguise may be achieved by using the following Pseudocode [10]:

For j=1 to 16 perform REj = LEj-1 ⊕ Pj;

LEj = F[REj] ⊕ REj-1;

LE17 = RE16 ⊕ P18;

RE17 = LE16 ⊕ P17;

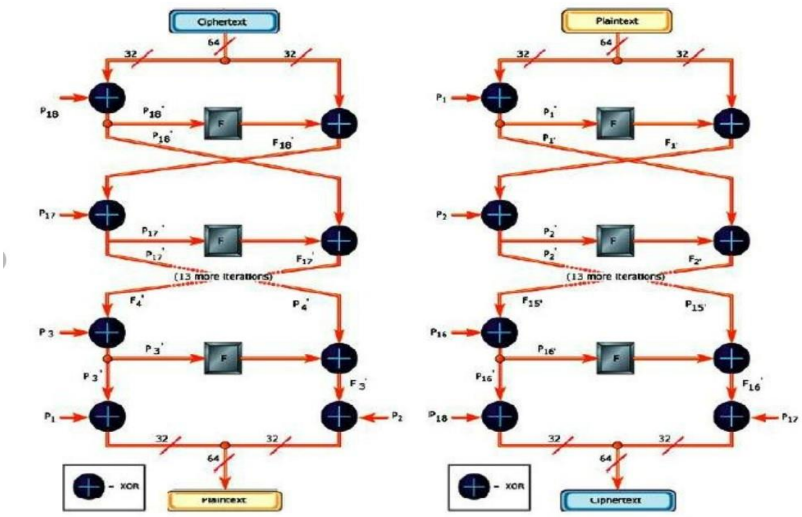


Figure 4: Blowfish algorithm in cryptography

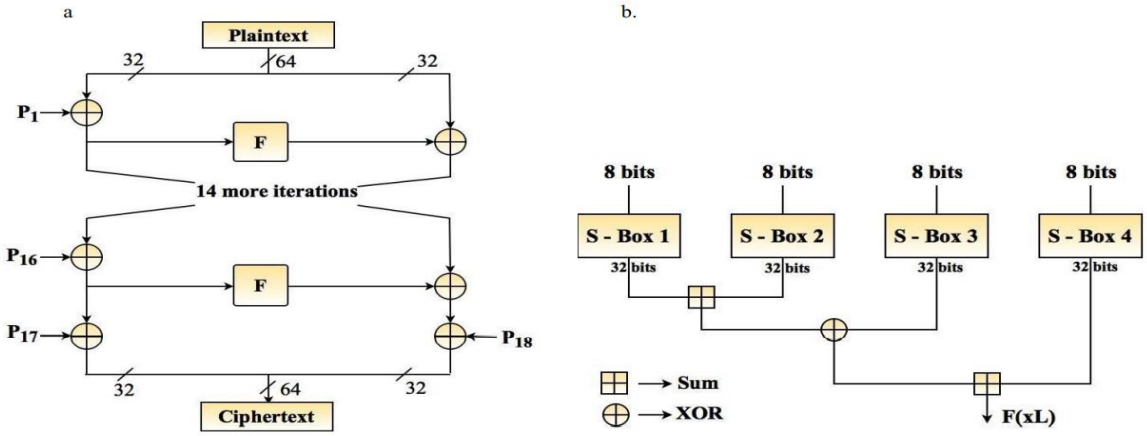
The only difference between encrypting and decrypting is that the P-array is used in the other direction during decryption. For this decipherment, we will use the following Pseudocode [10]:

For j=1 to 16 perform RDj = LDj-1 ⊕ P19-j ;

LDj = F[RDj] ⊕ RDj-1 ;

LD17 = RD16 ⊕ P1 ;

RD17 = LD16 ⊕ P2 ;



2.3.2 AES (ADVANCED ENCRYPTION STANDARD)

There are three distinct variations on the Advanced Encryption Standard (AES) algorithm: AES-128, AES-192, and AES-256. This arrangement depends on the sort of key utilized by the calculation all through the encoding and unraveling strategies. The pieces displayed here are the all out size of the key. As the size of the key develops, so does the level of safety The four rounds of encryption include of:

Step1: Substitute byte • Shift row • Mix columns • Add round key

Step2: While the decoding system is the converse of the encryption interaction, it actually requires:

Step3: Inverse shift row • Inverse substitute byte • Add round key • Inverse mix columns

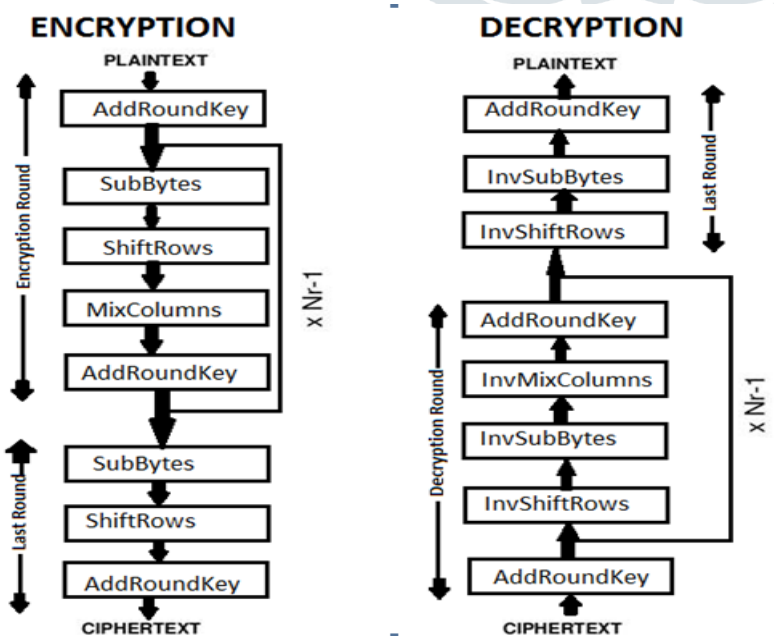
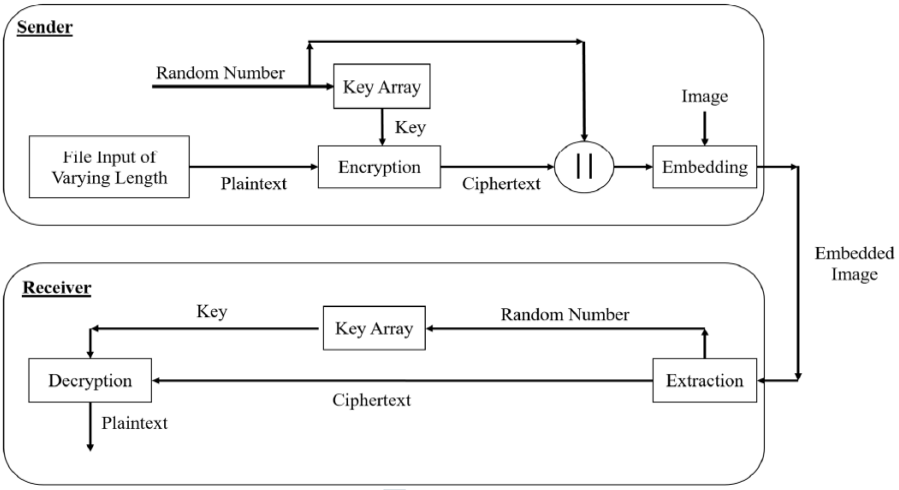


Figure 5. The AES cypher and decoding procedure

3. PROPOSED METHODOLOGY



One-way communication between a single sender and a single receiver is assumed throughout the work. the functional structure of the proposed work. shows the approach in action. The procedures are as follows:

The sender details, which might be rather lengthy, are saved in a file.

The length of the text not set in stone. Assuming the information length is under 64 pieces, zeros are added to the information. Once again, zeroes are added to the file if its size is more than 64 bits but not a multiple of 64. This file serves as input to an encryption block that applies the blowfish algorithm on its contents. Each sender and recipient has their own unique set of keys. For encryption, a key is chosen at random from a pool of possible keys. In order to protect the sensitive data included inside the file, a random key is chosen from the pool of keys contained within the encryption block, as described in (1). A ciphertext with a size that is a multiple of 64 bits is produced after the encryption block is complete.

Ciphertext = E (Plaintext, Key) (1)

The original file size (sender data) and the random number used to pick the encryption key are added to the ciphertext in the following format: (2). Information like this is what will be incorporated into the picture for authentication purposes.

Auth data = Random Number || size || Ciphertext (2)

4. ILLUSTRATION METHOD

The most un-critical pieces of various pixel values in the approved picture are currently different to mirror what might be compared to the information to be incorporated. During decryption on the receiving end, the picture in the extraction block is first analysed to determine the random number, size of the sender data, and cypher text. The retrieved random number is used to choose a decryption key from the pool of available keys.

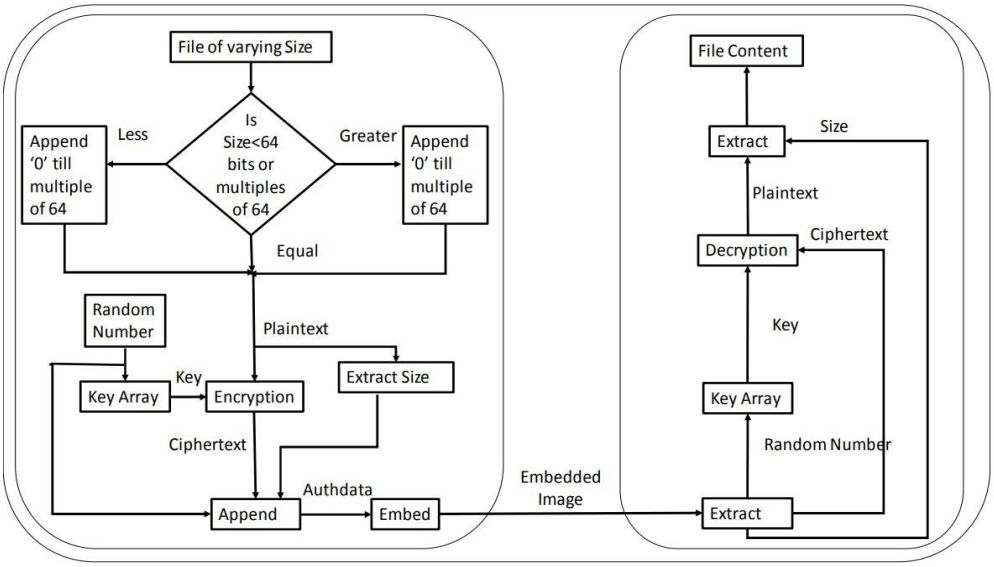


Figure 6: Process of illustration

a. Correction Factor

$$CF = \frac{T^2}{n}$$

Where T is total number of entries, n is total number of samples

b. Total Sum of squares

$$SS = \sum X_{ij}^2 - CF$$

Where, i= rows, j = columns and Xij is the mean.

c. Sum of squares between columns

$$SS_c = \sum_{j=1}^{n} \frac{T_j^2}{n_c} - \frac{T^2}{n}$$

DWhere n_c is number of colums.

d. Sum of squares between rows

$$SS_r = \sum_{j=1}^{n} \frac{T_j^2}{n_r} - \frac{T^2}{n}$$

Where n_r is number of rows.

e. Mean Square

$$MS = SS - (SS_r + SS_c)$$

f. Degree of Freedom

$$Df = \frac{SS}{MS}$$

g. F-Ratio

$$F_r = \frac{MS}{df}$$

5. EXPERIMENTAL RESULTS

I am dakshayini studying MTECH in JNTUK . ECE

Figure 7. Input text image

I am dakshayini studying MTECH in JNTUK. ECE

Figure 8. Output text image

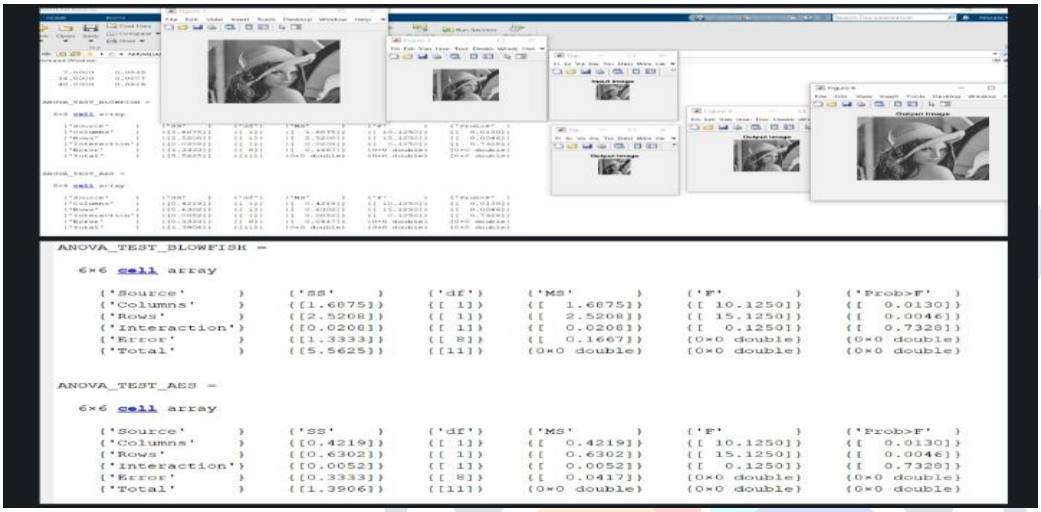


Figure 9. Different image ratios

{'Source' }	{'SS' }	{'df'}	{'MS' }	{'F' }	{'Prob>F' }
{'Columns' }	{[1.6875]}	{[1]}	{[1.6875]}	{[10.1250]}	{[0.0130]}
{'Rows' }	{[2.5208]}	{[1]}	{[2.5208]}	{[15.1250]}	{[0.0046]}
{'Interaction'}	{[0.0208]}	{[1]}	{[0.0208]}	{[0.1250]}	{[0.7328]}
{'Error' }	{[1.3333]}	{[8]}	{[0.1667]}	{0×0 double}	{0×0 double}
{'Total' }	{[5.5625]}	{[11]}	{0×0 double}	{0×0 double}	{0×0 double}

Figure 10. Results of Different image ratios of Blowfish algorithm

{'Source'}	{'SS'}	{'df'}	{'MS'}	{'F'}	{'Prob>F'}
{'Columns'}	{[0.4219]}	{[1]}	{[0.4219]}	{[10.1250]}	{[0.0130]}
{'Rows'}	{[0.6302]}	{[1]}	{[0.6302]}	{[15.1250]}	{[0.0046]}
{'Interaction'}	{[0.0052]}	{[1]}	{[0.0052]}	{[0.1250]}	{[0.7328]}
{'Error'}	{[0.3333]}	{[8]}	{[0.0417]}	{0×0 double}	{0×0 double}
{'Total'}	{[1.3906]}	{[11]}	{0×0 double}	{0×0 double}	{0×0 double}

Table 1: Results of Different images ratios of AES

time_blowfish =

7.0000	0.0338	0.1301	0.2480
16.0000	0.0355	0.1561	0.2790
40.0000	0.0372	0.1821	0.3100

time_AES =

7.0000	0.0487	0.2440	1.5320
16.0000	0.0512	0.2928	1.7235
40.0000	0.0536	0.3415	1.9150

Table 2: Comparison Table of TIME between blowfish and AES

6.CONCLUSION

A file with sender information of varying length is encrypted and decoded using the AES method in this study. The sender's information is encrypted before being included in the picture, so the attacker cannot read it in plaintext. The only way for an adversary to read the data without encryption is to decode it. An adversary can only decode data if they have both the encryption key and the algorithm. From the results, we may infer that files of any size can be encrypted and embedded in a specific picture, and that doing so has no appreciable impact on the execution time.

7. REFERENCES

[1] H. Liu and M. Steinebach, "Digital watermarking for image authentication with localization," in 2006 International Conference on Image Processing. IEEE, 2006, pp. 1973–1976.

[2] S. Tyagi, H. V. Singh, R. Agarwal, and S. K. Gangwar, "Digital watermarking techniques for security applications," in 2016 International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES). IEEE, 2016, pp. 379– 382.

[3] X.-L. Liu, C.-C. Lin, and S.-M. Yuan, "Blind dual watermarking for color images authentication and copyright protection," IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 5, pp. 1047–1055, 2016

[4] P. Jain and U. Ghanekar, "Robust watermarking technique for textured images," Procedia Computer Science, vol. 125, pp. 179–186, 2018

[5] P. Patil, P. Narayankar, D. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and BLOWFISH," Procedia Computer Science, vol. 78, pp. 617–624, 2016.

[6] A. A. Milad, Z. Muda, Z. A. B. M. Noh, and M. A. Algaet, "Comparative study of performance in cryptography algorithms (blowfish and skipjack)," Journal of Computer Science, vol. 8, no. 7, p. 91, 2012.

[7] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE). IEEE, 2014, pp. 83–93.

[8] Akshay, K. C., and Balachandra Muniyal. "Analysis of Execution Time for Encryption During Data Integrity Check in Cloud Environment," in International Symposium on Security in Computing and Communication, Springer, Singapore, 2018, pp. 617- 627.

[9] A. Alabaichi, F. Ahmad, and R. Mahmod, "Security analysis of blowfish algorithm," in 2013 Second International Conference on Informatics & Applications (ICIA). IEEE, 2013, pp. 12–18.

[10]W. Stallings, Cryptography and network security, 3/E. Pearson Education India, 2006.

[11]A. Tiwari and M. Sharma, "Novel watermarking scheme for image authentication using vector quantization approach," Radioelectronics and Communications Systems, vol. 60, no. 4, pp. 161–172, 2017.

[12]R. Saxena, K. Shah, R. Chawla, and V. Santhi, "Biometric watermarking for copyright protection of digital images," International Journal of Applied Engineering Research, vol. 9, no. 24, pp. 23 681–23 688, 2014.

[13]A. Kunhu, H. Al-Ahmad, and S. Al Mansoori, "A reversible watermarking scheme for ownership protection and authentication of medical images," in 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA). IEEE, 2017, pp. 1–4.

[14]M. Ramya, P. S. Soman, and L. Deepthi, "A novel approach for image security using reversible watermarking," in 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2017, pp. 338–343.

[15]C. R. Kothari, Research methodology: Methods and techniques. New Age International, 2004.