International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Enhanced authentication based security using TDES and MD5

Chirag Singh Sisodia[1], Aprajit Shrivastava[2]
[1]Dept.CSE,SRCEM Gwalior
[2]Assistant Professor (CSE), SRCEM, Gwalior

Abstract— For secure authentication over the internet and secure data transfer purposed using cryptography technique which provide high security. Encryption of an image, audio encryption, chaos based encryption contain various applications in numerous fields, concluding internet communication, transmission, medical imaging. Encryption is the most general method for image security promoting. Image encryption, video encryption, chaos centered encryption have functions in countless fields together with medical imaging, Tele-treatment and military communication, etc. in this paper using TDES and MD5 for secure authentication. In cryptography, firstly DES algorithm using for high security using 3DES and also called TDES. MD5 is an algorithm that's used to the data integrity authenticate with the aid in the production of a 128-bit message. Digest from information input (which may be an any length message) that is claimed to be as unique to that particular information. In this paper provide more security using TDES and MD5 on palm image.

Keywords— TDES; MD5; ECC; AES etc.

I. INTRODUCTION

The high performance in technology of networking leads usual values for interchanging of the data most drastically. Therefore the information has to be secure while transmitting it, Complex data, for example, credit cards, banking transactions and also social security numbers required to be protected. For this many encryption methods are current which are used to avoid the knowledge theft. In the wireless communication present day, data encryption performs a big role in information protecting by internet transmission focuses mostly on its security across the wireless. Encryption is a general method for promoting the information security [1].

Recently the information security has been a principal topic of digital data communications. These data could be highly secret and significant like military data, banking data, and multimedia contents such as image, audio, or video. This demands an effective cryptographic algorithms to secure these data transmissions from an unauthorized user revealing. Since the rapid developments in the field of computational processing speed become faster and faster. The attacks on the data are facilitated by such developments increases, and the challenge of securing the communications is now completely huge. Consequently, the used classical algorithms became highly weak to these kinds of threats. These threats inquire either new schemes or a kind of modification on the old ones to withstand the evolving attacks [2].

Verification of Biometric [3] is an automated method whereby an individual's identity is established through behavioral of investigative various characteristic or single trait of physiological, for example fingerprint, a signature, or retina. Traits of physiological are recognized characteristics, for example patterns of the iris and prints of palm. This type of measurement is basically permanent. A behavioral characteristic — for example, one's signature, voice, or keystroke dynamics — is influenced through both manageable movements and manageable factors of psychological. Because of behavioral characteristics can change over various times, registered biometric reference template must be updated each time it is used. Though biometrics, which is Behavior-based can less exclusive and less threatening to the users; physiological traits tend to suggestion superior security and accuracy.

Cryptography is the science and art of attaining protecting through encoding information to make them readable. Hence, it is additional data duplicating vulnerable and also hackers re-distributed. Therefore, the data have to be secure while transmitting it, sensitive data like banking transactions, credit cards and numbers of social security need to be secure. For this numerous encryption technique is a current which are used to avoid the knowledge theft. In present days of the wireless communication, the information encryption performs a major role in information securing in the online transmission focuses mostly on its security across the wireless [4].

II. BASIC SECURITY ISSUE

There are some basic security issue:

Authentication: - confirms authenticate person. It enforces that person is only one allowed to log on to his account

Authorization: - permits to person manipulate his resources in particular ways. This prevents a person from person growing balance account or deleting a bill.
Auditing: - deals with data hiding. It ensured person cannot spy on another person at the time of internet banking transactions.
Confidentiality (privacy) and integrity (trust): - protection in opposition to unauthorized know-how alteration
Availability: - protection in opposition to data removal or delays [5].

III. OVERVIEW OF SECURITY ALGORITHM

Some encryption approaches:

A. Data Encryption Standard (DES)

Primarily, key 56 bits are chosen from initial 64 through permuted choice. 56 bits are then separated into two different 28-bit halves, all half is there after preserved discretely. In successive rounds, each turned around halves are left via many bits and then 48 sub key bits are distinct with permuted option, 24 bits from left half and 24 from proper.

B. Advanced Encryption standard (AES)

It makes utilization of 10, 12, or 14 rounds. Size of key for example 128,192, or 256 bits, depends on numerous rounds. If the key and block are 192 bits, AES will attain 11 rounds of processing. If the key and block are 256 bits, then it achieves 13 processing rounds. AES is a non-Feistel figure [6] that decrypts and encrypts data 128 bits piece.

C. Triple DES

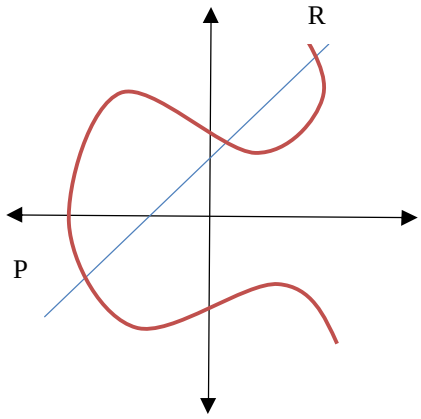
In cryptography, TDES is the general name for the TDES block cipher, which applies the DES cipher algorithm three different times to all data blocks. TDES provides a relatively simple technique of growing the DES key size to protect against various attacks. There are two keys using first is for encryption purpose and second for decryption purpose and last conclusion encrypted with the third key [6].

D. Elliptic Curve Cryptographic Algorithm (ECC)

The elliptic curve equation is given as,

$$\mathbf{Y^2 = x^3 + ax + b}$$

Where: a and b are elements of a finite field with pn elements, where p is a prime number which is picked as more noteworthy than 3. The some points set on curve is ordered pairs (x, y) set with coordinates in field and such that x and y content relative given through equation $\mathbf{Y^2 = x^3 + ax + b}$ defining the curve, plus an additional point that is said to be at infinity.



$y^2 = x^3+ax+b$

Fig. 1 Elliptic Curve Cryptographic

E. Key Generation

Key generation is significant part, where user has to produce private key and public key. The senders who want to send the data, he will first encrypt data with receiver‟s public key and also receiver will decrypt that ciphertext with its private key. Now, select a number„d‟ within a particular range of „n‟.

Applying following equation and create the general public key

Q=d*P

d = The random quantity that we have selected within the variety of (1 to n-1). P is the factor on a curve. „Q" is the public key and „d" is the private key.

Encryption

Let „m" be the data that are sending. Here to represent this information on the curve. Take into account the message „m" has the factor „M" on the curve „E". Now, randomly decide on value of „ok" from [1 – (n-1)]. C1 and C2 are to cipher textual content.

C1 = k*P

C2 = M + k*Q

Ciphertext C1 and C2 will be sent to the other user.

F. Decryption

Here, in this decryption process receiver will decrypt the ciphertext message with its own private key to get original message.

M = C2 – d * C1

G. Message Digest Algorithm 5

MD5 algorithm that is used to confirm data integrity by 128-bit MD5 creation of data input that is claimed to be as unique to that particular data.

The input information can be of any length or size, but output "hash value" size is always fixed.

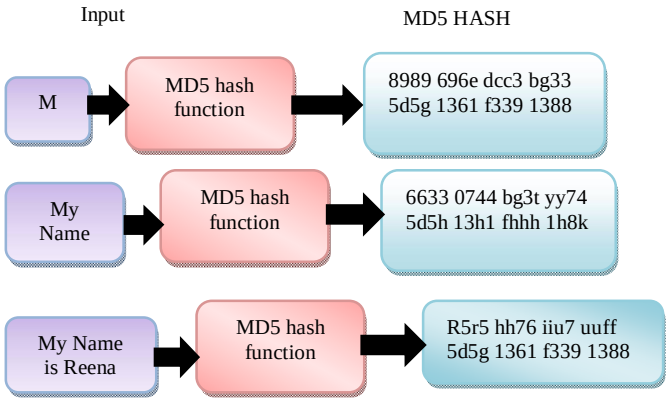


Fig. 2 Message Digest Algorithm 5

H. Here is an example of MD5 Hash function at work

The same thing applies even for information where each information that was sent and received can be confirmed applying the MD5 hash. The algorithm of MD5 is intended for applications of digital signature, where big file must be compressed in a protected method earlier being encrypted with the secret key under a public-key cryptosystem for example RSA [7].

IV. LITERATURE SURVEY

Boukhatem Mohammed Belkaid (2015) [8] et al present that Security of Data for end-end transmission is attained by numerous asymmetric and symmetric methods for data confidentiality, authentication of data and also exchange the key applying transport layer security. This paper presents a novel encryption technique for secure medical image transmission. The hybrid encryption method is based on the algorithms of AES and RSA. AES is used for confidentiality of expertise, the RSA is used for authentication and the integrity is certain of the fundamental function of correlation between adjoining pixels in the image. Our encryption system generates a unique password every new session of encryption. Several parameters were used for various tests of our analysis.

Mohamed A.

Seif Eldeen (2015) [9] et al present that DES was a prevalent symmetric key block cipher method. It was most general used algorithm of cryptographic. Security of DES's was an extremely debatable feature until it became not a secure algorithm in 1999. In this article, an improvement that overcomes security DES weakness is introduced. The alteration services chaotic logistic map and ECC art. The need key generation and distribution are also achieved through improvement to create session communication. Novel DES is applied on the procedures of image decryption and encryption. Experimental outcomes are carried out with complete analyses, the outcomes demonstrate that proposed method has an absolutely big key space to attack of brute-force and it has a

decent immunity to the statistical attacks. So the introduced novel algorithm of DES could be used as an unusually protect algorithm.

Aarti Devi (2015) [10] et al present that cryptography is an emerging methodology which is significant for network security. In present day world it is a crucial concern that while transfer image from one network to various networks over the internet, complete decryption and encryption should be practiced so that unlawful access can be prevented. For this we will survey related researches and done some problem identification. Based on our survey, we suggest some future suggestion which can be valuable for image encryption.

Ekta Chauhan (2015) [11] et al present that two most significant aspects of security that deal with transmitting information or data over various mediums for example Internet are encryption and steganography technique. Steganography deals with hiding data and encryption deals with hiding data plain text to unread data. Both of them are used to confirm security. AES is a variable bit block cipher and uses 128 bits variable length of the key. Here using steganography and AES for highly secure data transmission.

ROHITH S (2014) [12] et al present that created sequences are multiplied with 255 and bit through bit XOR operation employed on 8 bit LFSR states to find a final key sequence {Ki}. So obtained key sequence {Ki} is XORed with 8-bit grayscale image pixels {Pi} to found encrypted image. Proposed method performance is analyzed through computing Histogram, Entropy, Correlation and also MSE between encrypted and original image. This system has been validated for two 8-bit grayscale size 256×256 pixel images. The proposed method is compared with encryption/decryption applying a sequence {K1,i} generated applying logistic map. The histogram plot result of encrypted image applying proposed method is flat and consistently spread compared to the encryption approach applying a generated logistic map sequence. Also the correlation between adjacent encrypted image pixels found to be low.

Mr.Sudhanshu Suhas Gange (2014) [13] et al present that numerous methods use in the practice to provide copyright protection for example digital watermarking methods applying numerous transforms. Security can be provided through encryption and decryption method applying numerous approaches, for example RSA, AES, DES, etc. Here using encryption and digital watermarking for image security.

Rinki Pakshwar (2013) [14] et al present that numerous methods which are discovered from time to time to encrypt the images to create images extra secure. This paper presents a survey of over 25 research papers dealing with encryption method of an image scrambled the image pixels and also reduction correlation among pixels. In this paper a Survey of numerous Image Encryption and encryption approaches that are present is given. It moreover focuses on the Image encryption and decryption methods functionality.

V. PROPOSED WORK

A. TDES

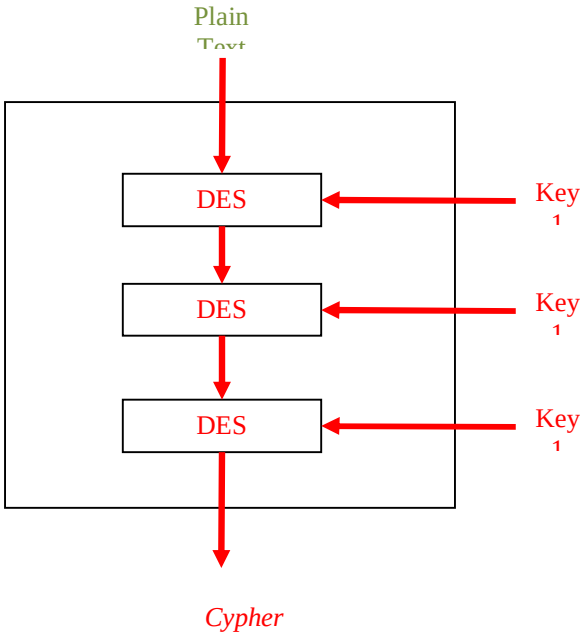


Fig. 3 Working of Triple DES

B. Algorithm

Run DES three times: ECB mode: If K2 = K3, this is DES Backwards compatibility Known not to be just DES with K4
Has 112 bits of security, not 3 56 = 168 algorithm if TDES uses 3 iterations of general DES ciphers. It gets a secret 168-bit key, which is separated into three different 56-bit keys.

1) Encryption with first secret key
2) Decryption with the second secret key
3) Encryption with the third secret key

Encryption: c = E3 (D2 (E1 (m)))
Decryption: m = D1 (E2 (D3(c)))
Applying decryption in the another step at the time of encryption provides backward compatibility with a general algorithm of DES..
c = E3 (D1 (E1 (m))) = E3 (m) c = E3 (D3 (E1 (m))) = E1 (m)
It is possible to use 3DES ciphers with a secret 112-bit key. In this case first and third secret keys are the same.
c = E1 (D2 (E1 (m)))

C. MD5

Algorithm of MD5 contain of 5 steps:

Step 1. Appending Padding Bits. Original data are "padded" (grown) so that size (in bits) is steady to 448, modulo 512. The cushioning standards are:

1) Original data are invariably padded with the one bit "1" first.

Then zero or extra bits "0" are padded to convey data size as much as 64 bits some than 512 more than one.

Step 2. Appending length. 64 bits are added to the end of the padded data to decide unique data length in bytes. The appending length rules are:

2) Original data length in bytes is converted to its binary 64 bits format. If overflow occurs, only the low-order 64 bits are used.

3) Break the 64-bit size into 2 words (32 bits each).

4) The low-order word is appended first and followed via high -order word.

Step 3. Initializing MD Buffer.MD5 algorithm need a 128-bit buffer with a particular initial value. The instating buffer tenets are:

5) The buffer is separated into 4 diverse words (32 bits all), named as A, B, C, and D.

6) Word A is initialized to: 0x67452301.

7) Word B is initialized to: 0xEFCDAB89.

8) Word C is initialized to: 0x98BADCFE.

9) Word D is initialized to: 0x10325476.

Step 4. Handling Message in 512-piece Blocks. This is the most important MD 5 algorithm step, which loops by appended and padded data in 512 bit blocks each. For all input blocks, 4 rounds of operations are achieved with 16 operations in all round.
Step 5. Output. The substance in buffer words A, B, C, D are back in grouping with low-arrange byte first.

D. Proposed algorithm:-

The encryption technique using MD5 or 3DES
Step1: count( ); // 128 bit from data
Step2: reduce() {
B = Convert 128 bit into 112 by deduct bits
from number who is multiple of 8 ; // parity chaking

}

Step3: apply 3DES(B) we get cipher text.

CT = 3DES(B);

The decryption technique using same algorithm.

Step1: receive(CT) {

B` = 3DES(CT); // decrypted algo of 3des text

}

Step2: apply hasing key (B`); // for getting original text

Step3: receive original message.

VI. RESULT SIMULATION

Base work

Fig. 4 Show user login id

If the user doesn't register first he/she clicked on register button is directly login.

Registration form

Fig. 5 Show user registration form

Whenever user register in our website for authentication we need his or her palm images so that we provide much and more security for the user.

After successful registration .

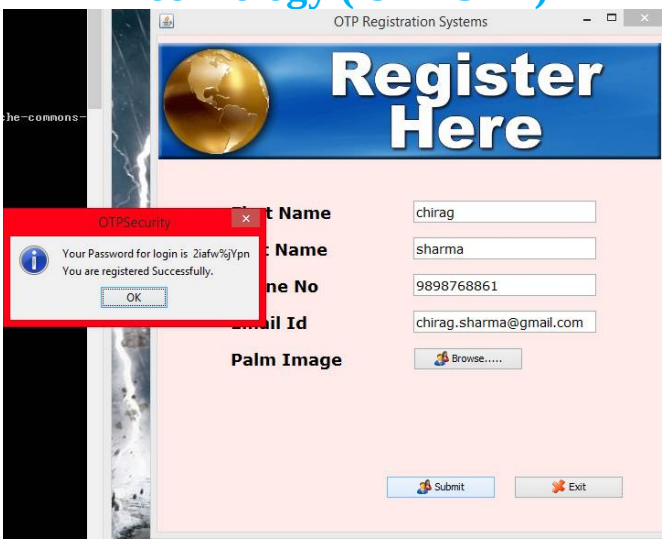


Fig. 6 Show user OTP security

We provide a password for the user.

When we login into the website it sends OTP for the user to provide security and after enter OTP web demand for palm image

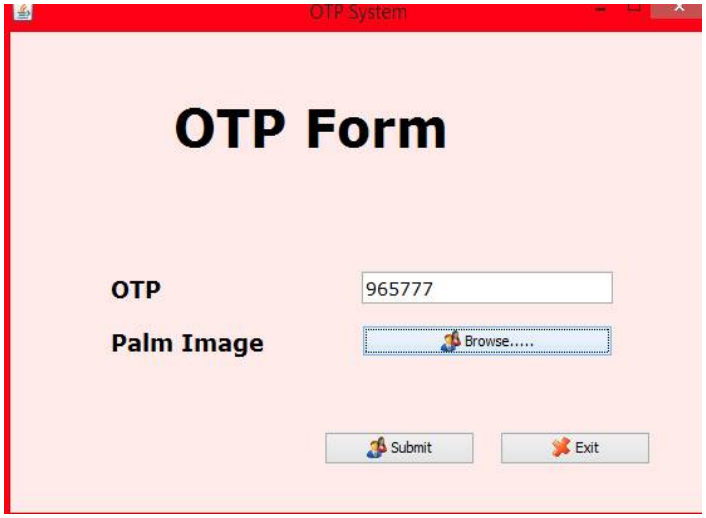


Fig. 7 Show fills user OTP security

After a successful login time consumed in whole process is shown in command window.

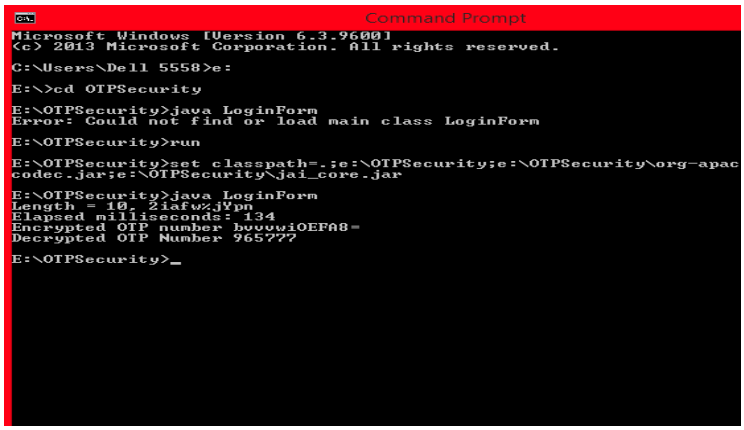


Fig. 8 Show successful login time consumed

Volume 4 Issue VII, July 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Proposed work

Fig. 9 Show proposed login

Fig. 10 Show user registration form

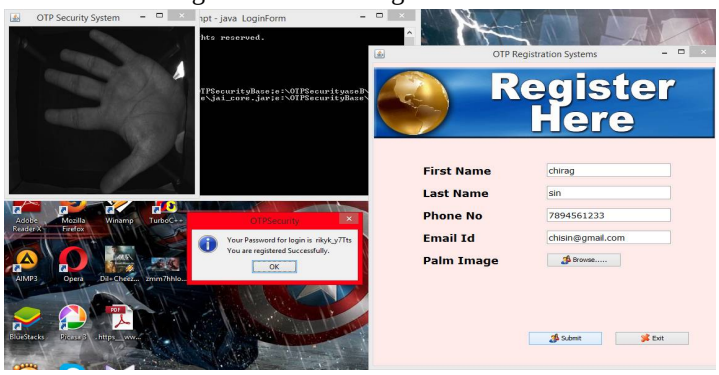


Fig. 11 Show user OTP security

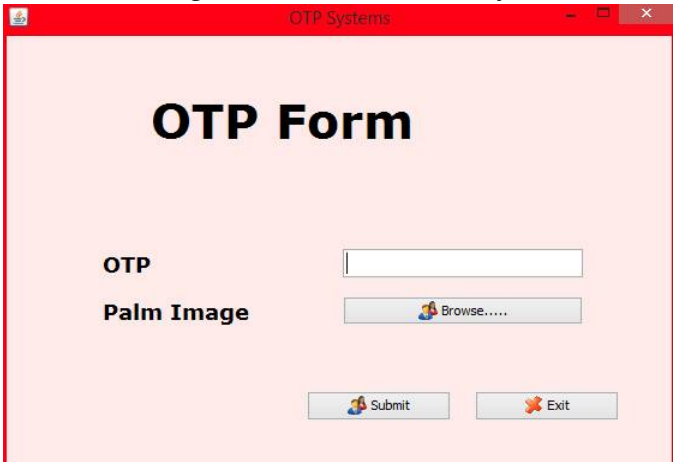


Fig. 12 Show user OTP form with palm image

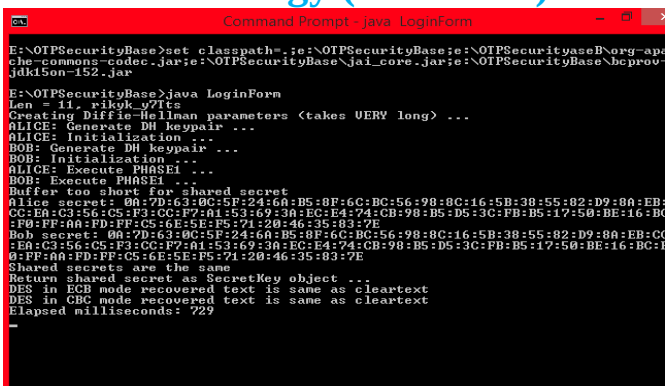


Fig. 13 Show proposed work successful login time consumed

VII. CONCLUSION

In this wireless world, the security for the data has become highly important for the communication by transmitting of digital products over the open network occur very frequently. In this paper, it has been surveyed that present works on the encryption methods here, using TDES and MD5 for enhanced security purpose on palm image. The high growing in networking technology lead a general culture for interchanging of the data very drastically We also discuss about the DES encryption techniques. Based on the above study, we provide the following future directions which can be helpful in better detection here can use Powerful encryption technique like DES and MD5. It can increase the size of the key also, so that a brute force attack is not simple. Random password initialization also helps it in the security improvement. Increasing the block size can improve the security. In this paper provide more security using TDES and MD5.

REFERENCES

[1] E. Thambiraja , G. Ramesh And Dr. R. Umarani ," Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012, pp: 226-233

[2] Mohamed A. Seif Eldeen, Dr. Abdellatif A. Elkouny and Prof. Dr. Salwah Elramly," DES Security Reinforcement Using Chaotic Logistic Map and Elliptic Curve Cryptography", 2015 IEEE.

[3] Ekta Chauhan and Prof. Unmukh Datta," Novel Approach to Secure Online Transaction using Stenography and AES in the Image", IJSRD - International Journal for Scientific Research & Development| Vol. 3, Issue 04, 2015 | ISSN (online): 2321-0613]

[4] Chauhan E," A Novel Technique Reduce Image Encryption And Decryption Time With Using Parallel Processing", E - Commerce for Future & Trends Volume 2, Issue 3 www.stmjournals.com, pp:1-8]

[5] Ekta Chauhan and Unmukh Datta," A Hybrid Technique to Secure E commerce Transaction with the Help of AES Encryption and Stenography in Image", International Journal of Hybrid Information Technology Vol.8, No.8 (2015), pp.271-278

[6] E. Surya and C.Diviya," Survey on Symmetric Key Encryption Algorithms", E Surya et al , International Journal of Computer Science & Communication Networks,Vol 2(4), 475-477

[7] Rukaiya Shaikh and Disha Deotale," A Survey on VANET Security using ECC, RSA & MD5", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015, pp: 167-172

[8] Boukhatem Mohammed Belkaid, Lahdir Mourad, Cherifi Mehdi and Ameur Soltane," Secure Transfer Of Medical Images Using Hybrid Encryption", 2015 IEEE]

[9] Mohamed A. Seif Eldeen, Dr. Abdellatif A. Elkouny and Prof. Dr. Salwah Elramly," DES Security Reinforcement Using Chaotic Logistic Map and Elliptic Curve Cryptography",2015 IEEE

[10] Aarti Devi, Ankush Sharma, Anamika Rangra," A survey on Symmetric Key Algorithms for Image Encryption", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 5, May 2015, pp: 2358- 2361

[11] Ekta Chauhan," Survey Paper on Improving Money Transaction Security Using AES and Steganography", International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 3, Issue 2, November (2015), pp: 65-69

[12] ROHITH S, K N HARI BHAT and A NANDINI SHARMA," Image Encryption and Decryption using Chaotic Key Sequence Generated by Sequence of Logistic Map and Sequence of States of Linear Feedback Shift Register",2014 ICAECC.

[13] Mr.Sudhanshu Suhas Gange and Prof.(Dr.).Ashok A.Ghatol," Combination of Encryption and Digital Watermarking Techniques used for Security and Copyright Protection of Still Image", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur India.

[14] Rinki Pakshwar, Vijay Kumar Trivedi and Vineet Richhariya," A Survey On Different Image Encryption and Decryption Techniques", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 113 – 116.

[15] SARANYA K, MOHANAPRIYA R and UDHAYAN J," A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014, pp: 539-544