ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Encrypted Image Message sending using Triple DES with Finger Print and MD5

Khushbu Soni[1], Shashi Sharma[2], Nagendra Kumar Sutilya[3]

M.Tech Scholar, Department of Computer Science, Jaipur Institute of Technology Group of Institutions, Jaipur Rajasthan, India[1]

Assistant Professor, Department of Computer Science, Jaipur Institute of Technology Group of Institutions, Jaipur Rajasthan, India[2]

M.Tech Scholar, Department of Computer Science, Jaipur Institute of Technology Group of Institutions, Jaipur Rajasthan, India [3]

ABSTRACT: Security is always the prime concern whenever transferring the text or any image message. In this paper we propose the unique concept of transferring the encrypted image , by first validating the user identity by validating the image of users in the database and then issuing the transaction it and encryption key for the session and then in the message sending phase the further finger print validation and comparison using the MD5 hash is performed0 to enhance the security and speed up the comparison process.

KEYWORDS: Cryptography, Encryption, Decryption, MD5 hash.

I.INTRODUCTION

Cryptography, a word with Greek beginning signifies "discharge composing", cryptography is the training and investigation of procedure for secure correspondence in nearness of outsiders correspondence with security so obscure individual neither access nor alter any data [29].

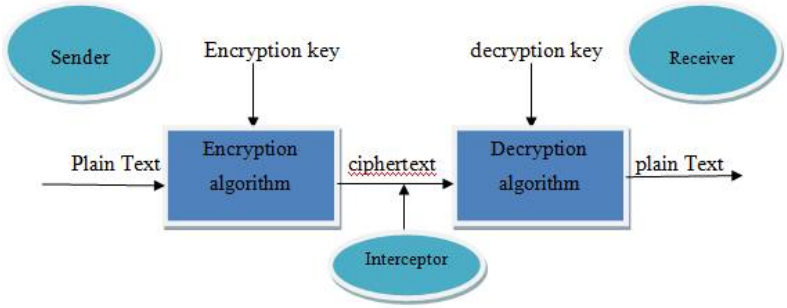


Figure 1.1 - Cryptography

Basic Terms Used In Cryptography -

Encryption - The way toward Encoding Plain Text message into cipher text message is called as Encryption.

Decryption - The turnaround procedure of changing cipher Text message back to plain text message is called Decryption.

Plain text - The first message, before being changed is called plain text as letter set, numeric particular image [4].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Cipher text-After the message is changed, it is called cipher text [4].

Key - Some critical information utilized by the cipher, known just to the sender and collector.

Goals of Encryption/Decryption

Confidentiality - In the PC the Information is transmitted ought to be gotten to just by the approved party.

Authentication - In this the character of the sender is to be checked by the system from the information got by any system whether the information is touching base from an approved individual or a false personality.

Integrity - In this exclusive the approved party is permitted to alter the transmitted information. Nobody else in the middle of the sender and collector are permitted to change the given message.

Non Repudiation - It guarantees that neither the sender, nor the recipient of message can preclude the transmission from securing messages.

Access Control - In this exclusive the approved gatherings are allow to get to the given information.

Types of Cryptography

Encryption and decryption changes over the first message in to non-coherent arrangement and sends the message over an uncertain channel. All networks are being introduced, interconnected to the worldwide network. The information is text, as well as sound picture and other multimedia pictures have been generally utilized as a part of our day by day life. The computerized pictures are normally utilized are spoken to in 2-D cluster.

There are fundamentally two sorts of cryptography

1. Symmetric or Secret Key Cryptography
2. Asymmetric or Public Key Cryptography

In Symmetric key cryptography, both the sender and beneficiary know a similar mystery code called key. Messages are scrambled by the sender utilizing the key and the beneficiary unscrambles it utilizing a similar key. E.g.: Data encryption standard (DES), Triple DES, Advanced Encryption Standard (AES) and Blowfish Encryption Algorithm.

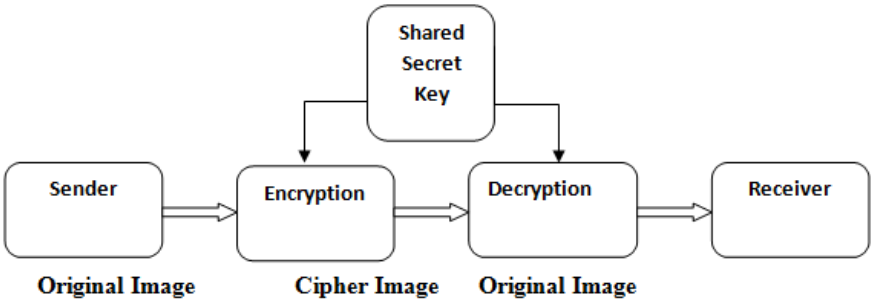


Figure 1: Symmetric Key Cryptography

In Asymmetric key cryptography, sender and beneficiary uses diverse key for encryption and decryption. The sender scrambles the data utilizing an open key and this key will be known by every one of the gatherings incorporated into the correspondence. The recipient unscrambles the data utilizing a private key and it ought to be kept as a mystery. E.g. RSA.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

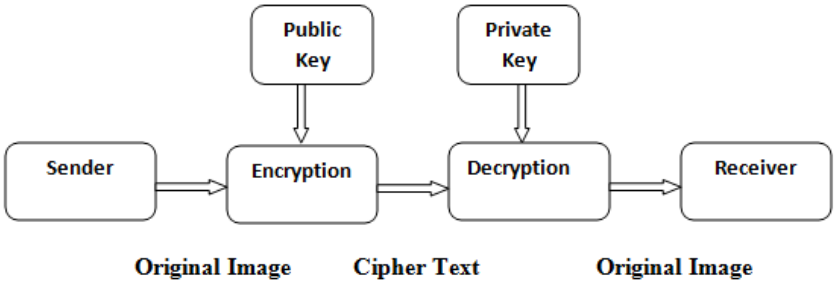


Figure 2: Asymmetric Key Cryptography

Encryption, the procedure utilized for changing the information into no readable frame for its security.

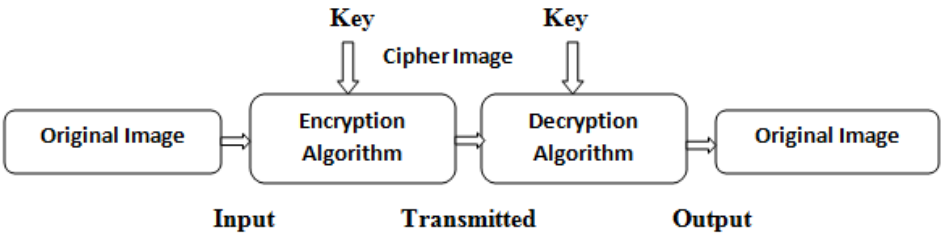


Figure 3: Encryption/ Decryption Algorithm

Picture encryption, the systems which is utilized to change over a picture to another which is difficult to get it. Then again, picture decryption is the system which recovers the first picture from the encoded picture. There are many picture encryption algorithms which are accessible, for example, DES, RSA, AES, Blowfish, and so forth however DES, RSA, AES have a few drawbacks so Blowfish algorithm and watermarking process for picture security is the best one.
The two unique sorts of mystery key cryptography are:

A. Block Cipher
Piece cipher, a deterministic algorithm which works on settled length gatherings of bits, called obstructs, with an un-fluctuating change that is indicated by a symmetric key. Square ciphers takes number of bits and after that scramble them as a solitary unit, cushioning the plaintext, so it is a multiple of the piece estimate. The normally utilized pieces estimate is of 64 bits.

B. Stream Cipher
Stream cipher, a symmetric key cipher where plaintext digits are consolidated with a pseudorandom cipher digit stream (key stream).In this kind of stream cipher, each plaintext digit is mixed every one thusly with the relating digit of the key stream, to give a digit of the figure content stream. It is in like manner called state figure because the encryption of each digit is liable to the present state.

II.TYPES OF ENCRYPTION TECHNIQUES

There are diverse sorts of encryption strategies which are utilized for the encryption of picture and data. The most widely recognized encryption systems are given as takes after:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

1. **RC2**

RC2is a piece cipher with 64-bits square cipher with a variable key size which go from 8 to128 bits. RC2 is defenseless against a related-key assault utilizing 234 picked plaintexts. RC2 is a square cipher that scrambles data in pieces of 64 bits.

RC2 is a symmetric piece cipher that works on 64 bit (8 byte) amounts. It utilizes a variable size key, however 128 piece (16 byte) key would regularly be viewed as great. It can be utilized as a part of the considerable number of modes that DES can be utilized. This algorithm grows a solitary message by up to 8 bytes.

2. **Advanced Encryption Standard (AES)**

AES was created by two researchers Vincent Rijmen and Joan in 2000. It utilizes the Rijndael square cipher. Rijndael key and square length can be 128, 192 or 256-bits. On the off chance that both the key-length and piece length are 128-piece, Rijndael will perform 9 handling rounds. In the event that the square or key is 192-piece, it performs 11 handling rounds. AES, Advanced Encryption Standard is a symmetric piece cipher that can scramble data squares of 128 bits utilizing symmetric keys 128, 192, or 256. AES encode the data pieces of 128 bits in 10, 12 and 14 round contingent upon the key size. Animal power assault is the main viable assault known against this algorithm. This encryption is quick and flexible. ; It can be actualized on different stages particularly in little devices.

3. **DES**

Data Encryption Standard, was to be recommended by NIST (National Institute of Standards and Technology).DES is 64 bits key size with 64 bits square size. 3DES is an update of DES; it is 64 bit square size with 192 bits key size. In this standard the encryption technique resembles the principal DES however associated 3 times to extend the encryption level and the ordinary safe time. 3DES is slower than other square figure strategies. 56-bit enter is utilized as a piece of DES and 16 cycle of each 48-bit sub keys are surrounded by permuting 56-bit key. Demand of sub keys is pivoted while unraveling and the indistinct algorithm is utilized. 64-bit piece evaluate is created utilizing L and R squares of 32-bit.

4. **Triple DES**

It essentially broadens the key size of DES by applying the algorithm three times in progression with three diverse keys. The consolidated key size is in this manner 168 bits which is3 times 56, which was past the scope of savage power.

5. **RC6**

RC6 has a piece size of 128 bits and it underpins key sizes of 128, 192 and 256 bits. It is fundamentally the same as RC5 in structure, utilizing data-subordinate pivots, and XOR operations and particular expansion; indeed, RC6 could be seen as entwining two parallel RC5 encryption forms. Be that as it may, RC6 uses an additional multiplication operation which was absent in RC5 with a specific end goal to make the pivot reliant on each piece in a word, and not only the slightest huge couple of bits.

6. **Blowfish**

Blowfish was planned in 1993 by Bruce Schneider. Blowfish is a symmetric key square cipher which utilizes a 64 bit piece size and variable key length. It takes a variable-length Key from 32 bits to 448 bits. It has variations of 14 rounds or less. The basic administrators of Blowfish algorithm comprise of table query, expansion and XOR. The table incorporates four S-boxes and a P-cluster. Blowfish is a figure in light of Feistel rounds, and the diagram of the F-work utilized means a change of the guidelines utilized as a piece of DES to give a comparative security more critical speed and profitability in programming. Blowfish is a snappy algorithm procedure and it can encode data on 32-bit microchips.

The Blowfish Algorithm:

Manipulates data in expansive pieces
Has a 64-bit square size.
Has an adaptable key, from 32 bits to no less than 256 bits.
Uses straightforward operations that are productive on microchips

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

e.g., select or, expansion, table query, secluded multiplication. It doesn't utilize variable-length moves or bit-wise stages, or contingent bounces.

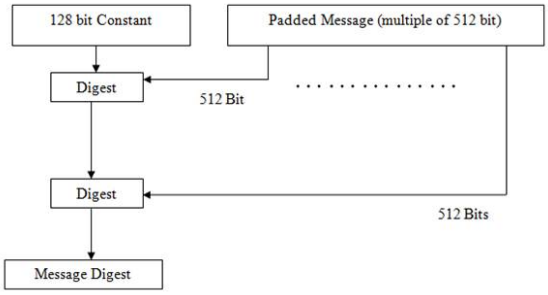
7. MD5 algorithm

MD5, and additionally MD2 and MD4, takes after a plan standard proposed by Merkle and Damagard. Its essential thought is to do hash in a piece shrewd mode. In a word, MD5 comprises of two phases: cushioning stage and pressure stage. In the cushioning stage, some additional bits (1 to 512bits) are annexed to the information message. The outcome bits is harmonious to 448 mod 512. At that point the length of the underlying message is changed to a 64-bit paired string(if the length is more noteworthy than 264, the lower 64-bit is utilized) and this 64 bits is added to the tail of the message as well. So the cushioning stage closes with a bit stream that comprises of at least one 512-piece squares. In the pressure stage, a pressure work is utilized on each 512-piece square and creates a 128-piece yield. The yield is constantly engaged with the computation of next round.

We start by assuming that we have a b-bit message as information, and that we wish to discover its message process. Here b is a subjective nonnegative whole number; b might be zero, it require not be a various of eight, and it might be self-assertively expansive. We envision the bits of the message recorded as takes after:

m_0 m_1 ... m_{b-1}

The accompanying five stages are performed to process the message process of the message.



III.ATTACKS AGAINST AUTHENTICATION MECHANISMS

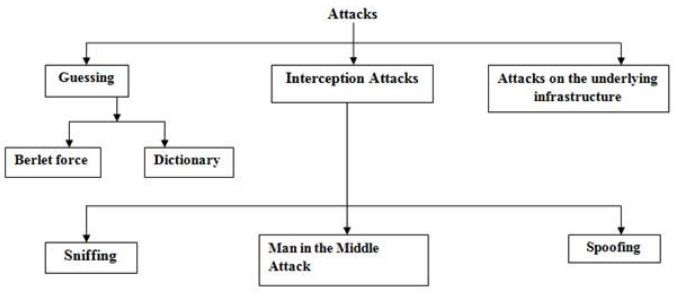


Figure 4: Classification of different kinds of attacks

A wealth of assaults is frequently conceivable to mount on any verification framework. There exists a greenery of inventive names for every single conceivable assault in particular settings. For instance the block attempt of a plaintext password, on the off chance that it is done while looking on a client writing it on a terminal, is called bear surfing

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

however when done over a system it is called password sniffing and so forth. This part will structure the assaults relying upon key likenesses between them.

A. **Guessing attack**

The point of a speculating assault is to utilize computational intends to find what the base-mystery is. It is a backhanded approach as in it can work regardless of the possibility that we are not possessing any type of the base-mystery. Asserting the base mystery may make the speculating more pragmatic yet that is the point of a capture attempt assault. This should be possible in pretty much wise ways. The two essential ideas of a speculating assault are the savage power approach and the lexicon approach.

B. **Brute force**

Most OS's utilization a devoted record or database where each username and the comparing password is put away. In current frameworks there is not the real password yet rather the cryptographic hash of the password that is put away with the username. This is to avoid anybody, having the capacity to recover the document, to take in all client passwords. Most validation instruments along these lines look at the cryptographic hash of the entered password as opposed to the plain content of it. An extra safety effort taken is to add an irregular steady to the password before hashing. This is known as a salt and will make the measure of blends for every password (two to the energy of the length of the salt) bigger.

C. **Dictionary**

The thought is to utilize a tremendous database of basic passwords and words and additionally blends of them and contrast their hash esteems and the ones put away in the password record. On the off chance that the aggressor finds a match he additionally has the relating password. In the event that the program used to contrast the hash esteems is capable with build every single conceivable blend of strings shorter than a limit esteem we in reality have a beast compel assault.

On the off chance that the assailant is not ready to recover the password document and the framework has a PC empowered interface the aggressor can even now utilize this sort of assault. Consider a site which requires a password to be entered in a frame. The aggressor could without much of a stretch compose a little program that posts effectively rounded out structures to the site utilizing an indistinguishable database from above. For this situation the plaintext password would be entered and not the hash estimation of the password. On the off chance that the site doesn't have any system to debilitate a client after a specific number of fizzled endeavors to login, this assault would at some point or another succeed.

With the equipment accessible on the typical desktop of today a fruitful word reference assault is hours away giving a 8-digit password. The ready availability of programs for this type of attack is frightening. LC5, John the ripper just to name a few. According to Schneier (2000) ”On a 400-MHz Quad Pentium II, L0phtcrack can try every alphanumeric password in 5.5 hours, every alphanumeric password with some common symbols in 45 hours, and every possible keyboard password in 480 hours.” Now imagine that was in 2000 and with desktops in 2004 having processors capable of over 1 GHz it doesn’t look good. The increasing speed of processors and hence the ability to reclaim hashed passwords have soon overrun the user’s ability to memories complex passwords.

IV.PROPOSED SOLUTION

In fig the user images are supplied with the encryption key to encrypt the image , and after that the valid and unique transaction key is generated , this done in order to validate the users involved in the transaction.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

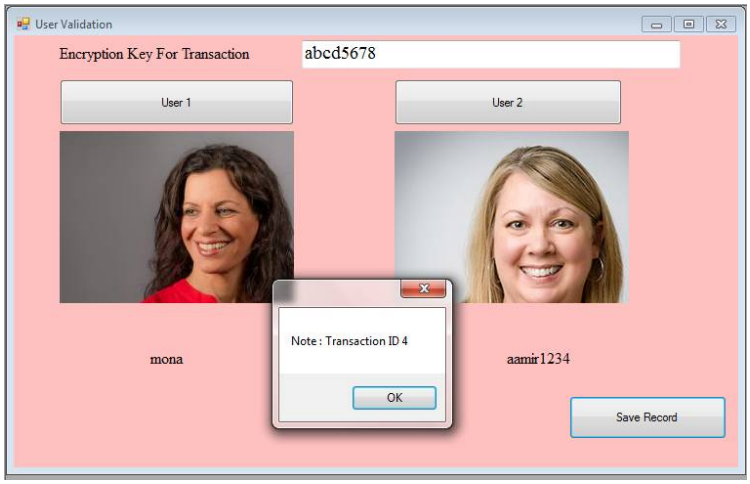


Figure 5: Validating the User

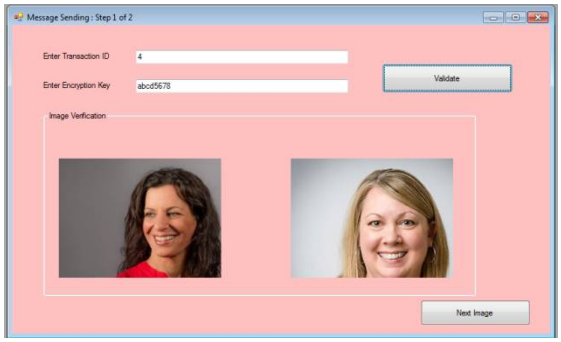


Figure 6 Message Sending step 1

In fig , the user have to first supply the valid transaction id and then the encryption key after that the user participating in the transaction are shown and after than the next step of the message sending will appear in the fig .
In fig , in order to cross validate the user the finger print are supplied and the finger print validation is done with the help of the MD5 Hash.

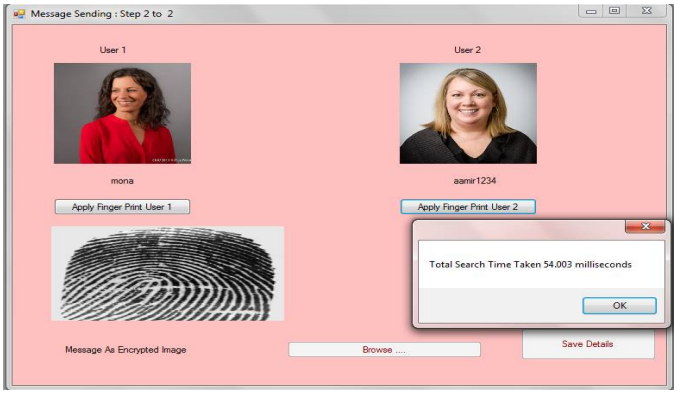


Figure 7 Finger Print validation

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

And after the finger print validation is done then the message is allowed to send. And the message is again an encrypted image which is to be send to the receiver.

V.CONCLUSION

Security of transaction is always an issue. And protecting the transaction information and validating the users is another issue.

The proposed work concluded that the time of the searching for image or the image comparison has reduced to the large extend as the MD5 comparison is faster than the pixel by pixel comparison. And the use of the finger print as well as the encrypted image has increased the security.

REFERENCES

1. Erfaneh Noorouzi, Amir Reza Est Akhrian Haghighi, Farzad Peyravi, Ahmad Khadem Zadeh, "A New Digital Signature Algorithm", 2009 International Conference on Machine Learning and Computing, Volume.3, IACSIT Press, Singapore, 2011.
2. Swarnendu Mukherjee, Debashis Ganguly and Somnath Naskar, "A New Generation Cryptographic Technique", International Journal of Computer Theory and Engineering, Volume. 1, No. 3, August, 2009.
3. Sameer Hasan Al-Bakri, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan and Gazi Mahabubul Alam, "Securing peer-to-peer mobile communications using public key cryptography: New security strategy", International Journal of the Physical Sciences Volume. 6, No.4, pp. 930-938, 18 February, 2011.
4. Challa Narasimham, Jayaram Pradhan, "Evaluation of Performance Characteristics of Cryptosystem Using Text Files", Journal of Theoretical and Applied Information Technology 2008.
5. Bruce Schneier, "Security Pitfalls in Cryptography", Counterpane Systems, 1998.
6. Prashant Kumar Koshta, Dr. Shailendra Singh Thakur, "A Novel Authenticity of an Image Using Visual Cryptography", International Journal of Computer Science and Network, Volume 1, Issue 2, April 2012.
7. J.M.Gnanasekar, V.Ramachandran, "Distributed Cryptographic Key Management for Mobile Agent Security", International Journal of Recent Trends in Engineering, Volume. 1, No.1, May 2009.
8. Fabian Monrose, Michael K. Reiter, Qi Li , Susanne Wetzel, "Cryptographic Key Generation from Voice", In Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.
9. Mina Mishra & V. H. Mankar, "Review on Chaotic Sequences Based Cryptography and Cryptanalysis", International Journal of Electronics Engineering, Volume.3, No.2, pp. 189– 194, 2011.
10. Katanyoo Klubsuwan, Surasak Mungsing, "Digital data security and hiding on virtual reality video 3D GIS", International Journal of Management Science and Engineering Management Volume. 4, No. 3, pp. 163-176,2009.