Photo and Fingerprint based modified Diffe-hellman algorithm for Message Transfer

Seema Choudhary[1], Amit Kumar Mishra[2]
[1]*M. Tech. Scholar, Sri Balaji College of Engineering and Technology, Jaipur Rajasthan.*
[2] *Sr. Lecturer and Head of Department, Computer Science, Sri Balaji College of Engineering and Technology, Jaipur Rajasthan*

Abstract- **Security of data transfer is always a issue. And it is always the utmost requirement to enhance the security. In our research paper we have create an approach of validating the user using the transaction key and finger print then message is transferred using the diffe-hellman approach . In order to validate the efficiency of our approach we compare the base pixel by pixel approach with the SHA approach of Image comparison and evaluated the approach in time efficiency Use of the SHA in the image comparison will result in reducing the time involved in the comparison of the finger print.**
The usage of photo and fingerprint has further enhanced the security and usage of SHA has speed use the comparison process.

Index Terms- **Cryptography, Diffe-hellman, Image Matching**

1.INTRODUCTION

Biometrics is mechanized techniques for distinguishing a man or checking the personality of a man in light of a physiological or behavioural trademark. Cases of physiological attributes incorporate hand or finger pictures, facial qualities, and iris acknowledgment. Behavioural qualities are characteristics that are found out or gained. Dynamic mark verification, speaker verification, and keystroke flow are cases of behavioural qualities. Biometric confirmation requires looking at an enlisted or selected biometric test (biometric layout or identifier) against a recently caught biometric test (for instance, a fingerprint caught amid a login). Amid Enrolment, as appeared in the photo beneath, a specimen of the biometric characteristic is caught, prepared by a PC, and put away for later examination. Biometric acknowledgment can be utilized as a part of Identification mode, where the biometric system distinguishes a man from the whole selected populace via scanning a database for a match construct exclusively in light of the biometric. For instance, a whole database can be looked to check a man has not connected for qualification benefits under two distinct names. This is now and then called ―one-to-many‖ matching. A system can likewise be utilized as a part of Verification mode, where the biometric system verifies a man's asserted personality from their already selected example. This is likewise called ―one-to-one‖ matching. In most PC access or network get to situations, verification mode would be utilized. A client enters a record, client name, or embeds a token, for example, a brilliant card, however as opposed to entering a secret key, a straightforward touch with a finger or a look at a camera is sufficient to confirm the client.

Patterns:

•The three fundamental examples of fingerprint edges are the curve, circle, and whorl:

•Arch: The edges enter from one side of the finger, ascend in the inside framing a circular segment, and after that leave the opposite side of the finger.

•Loop: The edges enter from one side of a finger, shape a bend, and afterward exit on that same side.

•Whorl: Ridges shape circularly around an essential issue on the finger.

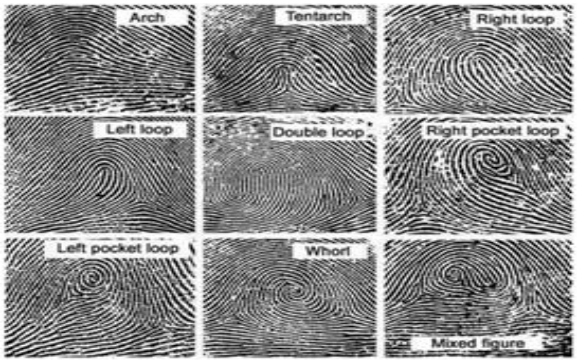

Fig 1. Finger Patterns

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].

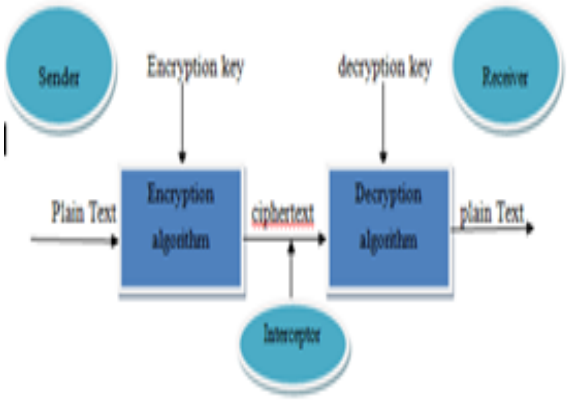

Fig 2 Cryptography

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].

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.

2. LITERATURE REVIEW

Vaibhav Poonia, Dr. Narendra Singh Yadav [8] Security has reliably been an amazing worry at whatever point there is correspondence amongst sender and recipient. To beat the issues of security ruptures various cryptographic calculations are utilized like: AES, DES, Triple DES, Blowfish, et cetera. The objective of this paper is to overhaul and evaluate the Blowfish count on the preface of various parameters like Encryption Quality, Correlation Coefficients, Key Sensitivity Test and Size of Output File. The =f' limit is changed by mixing the XOR and extension utilized as a piece of the main estimation. Four cases are made and examined. The results of the significant number of tests coordinated on these cases incite a normal conclusion that the security of the changed figuring with various cases makes the primary Blowfish computation more insignificant and more secure than the earlier.

Huy Hoang Ngo, Xianping Wu [9] In present day security models, cryptography assumes a basic part in ensuring data uprightness and classification in data systems. Be that as it may, cryptography itself is liable to cryptanalysis assaults. To diminish the cryptanalysis assault chance, a dynamic key hypothesis is exhibited and investigated in this paper. Since these dynamic keys are one-time utilized symmetric cryptographic keys, they can altogether enhance the security of cryptographic systems. The dynamic key hypothesis generation plan and key refresh component are formally broke down to exhibit adjust amongst security and execution. The hypothesis can be connected to improve the security and execution of cryptographic systems, particularly those utilized as a part of remote networks correspondence.

Md. Asif Mushtaque and Hash Dhiman [10] In this paper, they proposed our new symmetric key encryption count with decreased space diserse quality (AM Encryption Algorithm-AMEA).According to circle encryption hypothesis an encryption procedure should utilize not exactly or equivalent to the extent of the first document measure. There are two most critical parameters or attributes of calculation time and space. A calculation ought to require least time to play out their capacity and ought to have least space intricacy (space multifaceted nature as far as storage room after the encryption or the storage room required to store ciphertext). Diverse sorts of calculation has been outlined some of them gives better security yet the space many-sided quality of all current calculation is high. In this way, we proposed another cryptographic calculation in view of symmetric key stream figure that furnishes better security with least space multifaceted nature. This calculation is not same as past stream figure calculation (the most usually utilized RC4) it has some new elements, for example, Random Key Selection with transposition that gives better security.

Maulik P. Chaudhari and Sanjay R. Patel [11] Another paper is "A Survey on Cryptography Algorithms" Maulik P. Chaudhari and Sanjay R.

Patel.This paper talks about in subtle elements the prerequisite of the cryptographic calculation in the field of the data security. In this paper the creator has talked about in points of interest plaintext attack[11] against a decreased round variation of blowfish that is made less demanding by the utilization of powerless key.Blowfish is more secure and quick handling calculation. In any case, in this paper the creator likewise distinguished some issue in the current Blowfish calculation i.e. the blowfish feeble keys produces "terrible" S-boxes.

Josef Steinberger , and KarelJežek [14] In this paper the creator has talked about Blowfish calculation, that it is a variable-length key piece figure. What's more, in this he have depicted in points of interest the working of the blowfish calculation and applications where the blowfish calculation is used.For this paper we get the thought in regards to the procedure which is adjusted in the encryption and decoding utilizing the blowfish calculation. The data which we get from this paper are as per the following, the key size which is utilized for encryption and in the unscrambling procedure and rounds which are performed in the data encryption and last yield which we get from that.

3. DESIGN AND METHODS

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:

3.1 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.

3.2 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.

3.3DES

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.

3.4 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.

3.5 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.

3.6 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.

Blowfish gives the workplace to empower anyone to utilize encryption free of licenses and copyrights. No ambush is known to be productive against blowfish, while it encounters weak keys issue (Bruce, 1996) .Blowfish is unpatented, allow free, and it is sans open of cost for all livelihoods. Blowfish has varieties of 14 rounds or less. It is successor to Twofish.

3.7 Diffie-Hellman Protocol

The Diffie-Hellman convention is a technique for two PC users to produce a common private key with which they would then be able to trade information over a shaky channel. Give the users a chance to be named Alice and Bob. First, they agree on two prime numbers and , where is large (typically at least 512 bits) and is a primitive root modulo . (In practice, it is a good idea to choose such that is also prime.) The numbers and need not be kept secret from other users. Now Alice chooses a large random number as her private key and Bob similarly chooses a large number . Alice then computes , which she sends to Bob, and Bob computes , which he sends to Alice.

Now both Alice and Bob compute their shared key, which Alice computes as and Bob computes as

Alice and Bob can now use their shared key to exchange information without worrying about other users obtaining this information. In order for a potential eavesdropper (Eve) to do so, she would first need to obtain knowing only , , and .

This can be done by computing from and from . This is the discrete logarithm problem, which is computationally infeasible for large . Computing the discrete logarithm of a number modulo takes roughly the same amount of time as factoring the product of two primes the same size as , which is what the security of the RSA cryptosystem relies on. Thus, the Diffie-Hellman protocol is roughly as secure as RSA.

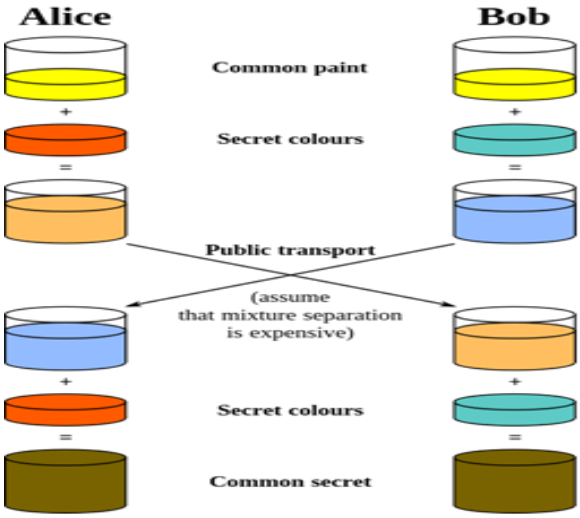

Fig 3 Diffie-Hellman Protocol

3.8 SHA-1 Function

In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash work planned by the United States National Security Agency and is a U.S. Government Information Processing Standard distributed by the United States NIST. SHA-1 creates a 160-piece (20-byte) hash esteem known as a message process. A SHA-1 hash esteem is normally rendered as a hexadecimal number, 40 digits in length.

3.9 Technologies Used

Eclipse is an integrated advancement environment (IDE) utilized as a part of computer programming, and is the most broadly utilized Java IDE. It contains a base workspace and an extensible module framework for re-trying the environment. Eclipse is composed generally in Java and its essential utilize is for creating Java applications, yet it might in like way be utilized to create applications in other programming dialects by techniques for modules, including Ada, ABAP, C, C++, COBOL, D, Fortran, Haskell, JavaScript, Julia,Lasso, Lua, NATURAL, Perl, PHP, Prolog, Python, R, Ruby (checking Ruby on Rails system), Rust, Scala, Clojure, Groovy, Scheme, and Erlang. It can in like way be utilized to create records with LaTeX (by techniques for a TeXlipse module) and bundles for the product Mathematica. Advancement environments incorporate the Eclipse Java improvement mechanical assemblies (JDT) for Java and Scala, Eclipse CDT for C/C++, and Eclipse PDT for PHP, among others.

Swing is a GUI gadget instrument stash for Java. It is a piece of Oracle's Java Foundation Classes (JFC) – an API for giving a graphical UI (GUI) for Java programs.

Swing was produced to give a more advanced course of action of GUI parts than the prior Abstract Window Toolkit (AWT). Swing gives a neighborhood look and feel that copies the look and feel of a few stages, and moreover supports a pluggable look and feel that engages applications to watch and feel inconsequential to the hidden stage.

4. ALGORITHMS

The project flow consists of following

1.User Validation

In the user validation, we will select the photo of the user1 and user 2 involved in the sending process. The photos are then validated in the user's databases and the username is fetched. After that using the blowfish encryption algorithms the image are encrypted and send. A long with that a unique transaction key and encryption key is stored in database. Encryption key will act us key to encrypt images .

Fig4: Validation Photo

Algorithm for User Validation

Step 1: Specify the Encryption Key

Step 2: Specify the user 1 image and the database checking will be automatically performed by checking the photo in the database.

Step 3: Encrypt the Image of user 1 using the encryption key provided.

Step 4: Specify the user 2 image and the database checking will be automatically performed by checking the photo in the database.

Step 5: Encrypt the Image of user 2 using the encryption key provided.

Step 6: Save the record of transaction in the database and the truncation id.

2. Message Exchange

This process is divided in two parts.

(a)User Validation (b) Message Sending

User Validation: Firstly we will enter the transaction key and key for encrypting image. The entires are validated from databases and then images are decrypted and shown on screen, then only we can proceed to message sending step.

Fig5: Message sending

B. Message Sending: Now finger prints are input and unique random number an basis of finger print is generated and message is sent or exchanged using the diffie-hellmam algorithms.

Algorithm for Message Sending

Step 1: Specify the Encryption Key and transaction id.

Step 2: Validate the Encryption Key and transaction key in the database.

Step 3: Image of the users participating in the transaction will get displayed.

Step 4: Proceed to the next step of the message sending.

Step 5: Specify the Finger print and validate with the user finger print in the database using the SHA algorithm.

Step 6: Send the message using the differ-hellmam algorithm.

5. IMPLEMENTATION

In the message sending, the transaction key and the encryption key is required to be entered by the user and after that the users interaction images will be shown.

Fig 6 Transaction Key and Encryption Key Entry

The validation of the finger print, and send the message from user 1 to user 2 using the Diffe –

Hellman algorithm. The user 1 is first required to enter the finger print details and then the finger print is validated in the database using the SHA-1 concept and after that the user 2 is required to submit the finger print which is again validated in the database using the SHA-1 algorithm and then the Diffe-Hellman algorithm is followed for the message exchange.

Fig 7 Message Exchange Form.

6. IMPLEMENTATION

Case I: User 1 and User 2 interacting data

Fig 8 SHA-1 Comparison Proposed Work Case I

The Fig 8. Shows the proposed algorithm implementation using SHA-1 implementation and the shows the number of milliseconds required to complete the comparison.

Fig 9 Base Work Case I

In Fig 9, the time analysis of the base approach using the pixel by pixel analysis.

	Pixel By Pixel Approach	Proposed Work
USER 1 AND USER2	401 ms	146 ms

Table 1 Time comparison table for case I

The Table 1, shows the comparison between the base approach and the SHA1 based proposed approach. it shows that the Proposed work have reduced the comparison time to the considerable extent.

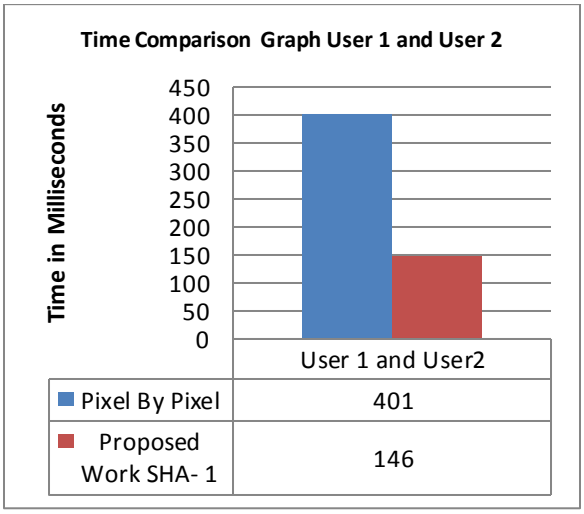

Fig10 Time comparison graph case I

The Fig 10 show the comparison graph between two approaches, using the Bar graph together with the tables showing the time differences.

7. CONCLUSION

Security is the main concern in the transaction, the proposed dissertation has increased security be encrypting the photos of user interacting in the transaction and the encrypted images are first decrypted at the time of the sending of message and after the encryption and transaction key validated then the message are further transferred. Using the SHA in the image comparison will speed up the process of image comparison, thus the security and speed both has enhanced.

8. REFERENCES

[1] Vaibhav Poonia, Dr. Narendra Singh Yadav,"Analysis of modified Blowfish Algorithm in different cases with various

parameters",International Journal of Engineering Research and General Science Volume 3, Issue 1,January-February, 2015.

[2] Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, "Dynamic Key Cryptography and Applications",International Journal of Network Security, Vol.10, No.3, PP.161–174, May 2010.

[3] Maulik P. Chaudhari and Sanjay R. Patel,"International Journal of Advance Research in Computer Science and Management Studies",International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 3, March2014 pg.100-104.

[4] Pratap Chandra Mandal,"Dimensions Affecting Customer Satisfaction in Retail Banking: A Review",Vol. 2, Issue 1, pp: (35-40), Month: January - April 2015.

[5] Josef Steinberger , and KarelJežek,"Automatic Text Summarization",Znalosti 2008, pp. 1–12, 2008.

[6] Yuh-Rau Wang, et. Al,"A blind watermarking method using maximum wavelet coefficient quantization",November 2009.

[7] A. G. Reddy et. Al,"Y-chromosome evidence suggests a common paternal heritage of Austro-Asiatic populations",2007 Mar 28.

[8] D. He et. Al,"Virtual Currencies and Beyond: Initial Considerations".

[9] Feng Fujun et. al,"The influence of Laval nozzle throat size on supersonic molecular beam injection",June 2014, Volume 22, Issue 2, pp 118–121.

[10] Nisha H. Motwani,"Trophic complexity of zooplankton–cyanobacteriainteractions in the Baltic Sea:Insights from molecular diet analysis",2015.

[11] V. Purushothaman and S. Sreedhar, "An improved secret sharing using XOR-based Visual Cryptography," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, 2016, pp. 1-4.

[12] R. M. Shiny, P. Jayalakshmi, A. Rajakrishnammal, T. Sivaprabha and R. Abirami, "An efficient tagged visual cryptography for color images," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, 2016, pp. 1-4.

[13] S.Sridevi sathya Priya,P.Karthigai Kumar, N.M. SivaMangai, V.Rejula "FPGA Implementation of Efficient AES Encryption "IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15 978-1-4799-6818-3/ 15/ $31.00 © 2015 IEEE

[14] JG pandey, S gurunarayan "Architectures and Algorithms for Image and Video Processing using FPGA-based Platform "978-1-4799-4006-6/14/$31.00 ©2014 IEEE

[15] Vakkayil Megha Gopinath "MAES Base Data Encryption and Description Using VHDL" © 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939

[16] Cryptography The art of Hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Volume 2, Issue 12, December 2013.

[17] Irfan Landge et al., "Encryption and Decryption of Data Using Twofish Algorithm", World Journal of Science and Technology, ISSN: 2231-2587, Vol. 2, No. 3, pp. 157-161, 2012.

[18] Anjali Arora et al., "A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers", International Journal of Computer Science and Information Technology & Security, ISSN: 2249-9555, Vol. 2, No. 2, April 2012.

[19] A. Grediaga et al., "Analysis and Implementation Hardware-Software of Rijindael Encryption", IEEE Latin America Transactions, Vol. 8, No. 1, pp. 82-87, March 2010.

[20] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 15, 2010