ISSN No:-2456-2165

Secure Live ATM Transaction using Steganography and Image Processing

[1]Krishnanand
Computer Science and Engineering
SRM Institute of Science & Technology
Chennai, India

[2]E. Saraswathi
Computer Science and Engineering
SRM Institute of Science & Technology
Chennai, India

[3]Ritesh Singh
Computer Science and Engineering
SRM Institute of Science & Technology
Chennai, India

[4]Shubham Nandi
Computer Science and Engineering
SRM Institute of Science & Technology
Chennai, India

Abstract:- The Current banking system is very popular with the feature of offering customers a high-quality service 24 hours a day, but the major issue in banking is the authenticity of the customer and most systems today rely on static passwords to verify a user's identity. The user always tries to use, easy and guessable passwords, try to use the same password for one or more accounts, or some will write down their password, etc. So, there are many ways to steal these passwords by a hacker, they will be using many techniques, such as peeping i.e., shoulder surfing, snooping, sniffing, etc. Also, the PIN validation is done at later stages of ATM transactions. However, such passwords, come with major security concerns. The crucial prerequisite these days is to get rid of the various forms of attacks. Due to this reason, different biometric systems gain popularity worldwide for their behavior and physiological features. However, the current biometric systems, for example, iris, palm, face fingerprints or voice are extremely complex and increase the time for each transaction. To overcome these issues a new concept has been proposed in this paper by Using steganographic and visual cryptography technique approach on image processing with the help of mobile phone. The proposed system uses live ATM transaction with steganography to generate dynamic pin for each new ATM transaction performed. The concept of 4-digit static pin is eliminated with the 4-digit dynamic pin. Whenever a transaction is performed a random 4-digit pin will be generated by the server and it will be steganographic with an image which will be visible to user on his mobile screen. The user needs to type their profile password and the encrypted pin in the image will be visible and can be used to perform transection. In case of 3 wrong attempts the image of the person who is performing the transaction will be captured and the alert system will send alert messages to user's main and alternate mobile number.

I. INTRODUCTION

The advancement of the payment system in the modern world has gone passed cash to cheques, and then to payment cards such as credit cards and debit cards. ATM stands for Automated Teller Machine. It is a telecommunications tool that enables customers to make financial transactions, especially withdrawals, without the need for a cashier, clerk, or bank accountant. Along with the easy and feasible use of ATMs, there has also been an increase in the number of ATM thefts and frauds, which are growing at an appalling rate. ATM card verification methods have changed little since they were first introduced in the 1960s. ATM safety standards are largely found in the safety traps of magnetic resources. The data on the magnetic stripe are usually coded using two or three tracks, because, it is not difficult or expensive to have the equipment to encode magnetic stripes. The standard covering this area is International Organization for Standardization (ISO) 7811 and the technique for writing of the tracks is known as Friend-to-friend (F/2F). Thankfully, magnetic stripe feebleness has been partly addressed by the introduction of Europay International, MasterCard and Visa (EMV) smartcards.

Currently the ATM communicates with central host processor by Internet Service Supplier that includes a gateway where all the ATM networks offered to the user. The ATM Machine is connected to the central host processor using a modem. Once the client desire to perform transection offers a PIN and ATM card. ATM machine forwards to the central host processor whereas ATM request to the customer bank. If client request a money central host processor initiates electronic fund transfer from client bank to ATM central host processor account. Once the transfer is completed to the central host processor it sends permission to the ATM to withdraw the money.

Despite the many warnings given by the card user, many people continue to choose easily guessable passwords and PINs such as phone number, date of birth, social security number etc. However, due to the limitations of this design, an intruder with a user card can access the user's PIN one in every 10,000 users will have same number. If the users have more than one cards, all the PINs needs to be memorized by the user. This can lead user to write or save the passwords physically or use same passwords that can be found in the dictionaries. A notable example of this was shown by Klein, who could crack 25% of 14,000 passwords using a dictionary attack with only 86,000 words.

ISSN No:-2456-2165

The reason for not going with the encryption method is because the encryption creates a coded message that can be

easily identified by the hackers that some important information is being transferred as we know this whole process will be completely relied on the internet hence, we tried to eliminate these threats by shifting to more tradition algorithm that is steganography.

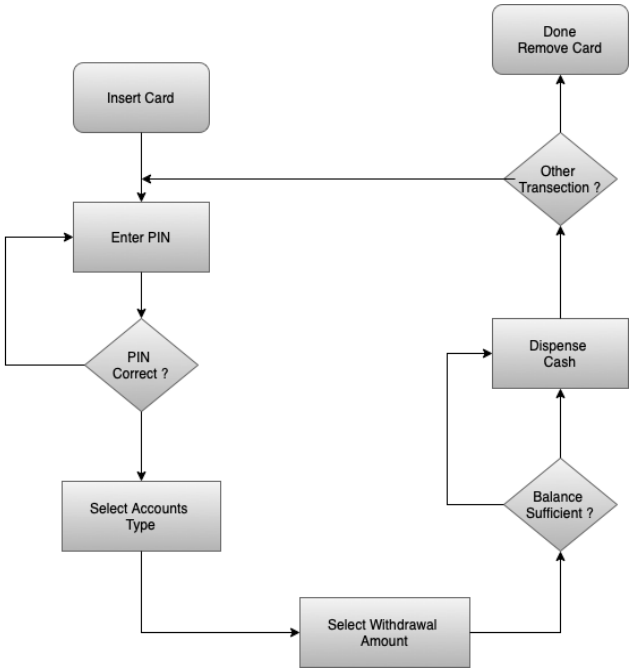

Fig 1 Traditional ATM cash withdrawal Process Flowchart

The Proposed system uses live ATM transaction with steganography to generate dynamic pin for each new ATM transaction performed. The concept of 4-digit static pin is eliminated with the 4-digit dynamic pin. Whenever a transaction is performed a random 4-digit pin will be generated by the server and it will be steganography with an image which will be visible to user on his mobile screen. The user needs to type their profile password and the encrypted pin in the image will be visible and can be used to perform transection. In case of 3 wrong attempts the image of the person who is performing the transaction will be captured and the alert system will send alert messages to user's main and alternate mobile number.

The reason for not going with the encryption method is because the encryption creates a coded message that can be easily identified by the hackers that some important information is being transferred as we know this whole process will be completely relied on the internet hence, we tried to eliminate these threats by shifting to more tradition algorithm that is steganography.

➢ *STEGANOGRAPHY Types*

STEGANOGRAPHY is derived from the Greek Words: STEGANOS - "Covered" and GRAPHIE – "Writing". The main goal of the steganography is to make communication between two or more ends in completely undetectable manner without drawing suspicion to the transmission of the hidden data. This is not done to keep the information hidden from others, but it is to keep others from thinking that the information even exists. The data can be mainly in basic formats like:

- *Audio Steganography:*

Information hiding technique is a new kind of secret communication technology and Audio Steganography is science of hiding messages or audios by modifying an audio signal in an imperceptible manner. The host message before steganography and the stego message after steganography should have similar features. Embedding secret messages on digital audio is a very difficult process. A variety of techniques for embedding information into digital audio have been developed.

- *Image Steganography:*

As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called a cover photo and the image obtained after steganography is called a stego image. The standard image algorithm for steganography is the LSB embedding algorithm.

- *Video Steganography:*

Steganography can also be used in video files. If we hide information in a video file, it can be called Video Steganography. The video file should not be seen by the attacker. The video steganography is divided into three categories: intra embedding, pre embedding, and post embedding. Intra embedding methods are categorized into video compression categories such as intra-prediction prediction, motion vectors, pixel translation, converting coefficients. Pre-embedded methods are used in raw video, which can be categorized and convert domains. Post-embedding methods are more focused on bitstreams, which means that the process of embedding, and extraction of steganography video is all used in small, compressed streams.

- *Text files Steganography:*

Steganography can also be used in text files as well. When we hide information in a text file, it is called Text Steganography.

➢ *LSB Methods*

In the gray scale picture, each pixel is represented by 8 bits. The last pixel bit is called the Least Significant bit as its value will only affect the pixel value by "1". Thus, this structure is used to hide data in the image. If anyone thought of the last two pieces as LSB pieces as they would only affect the pixel value by "3". This helps to store additional data. Steganography of Bit Least Significant Bit (LSB) is one such method where the insignificant bit of imagery is replaced by data bit. As this method is vulnerable to steganalysis to make it more secure we encrypt raw data before embedding it in the image. Although the encryption process increases the complexity of the time, but at the same time it also provides higher security as well. This method is very simple. In this way some important bits or all the bits inside the image are replaced with fragments of private message. The LSB

embedding method has become the basis of many strategies that hide messages within multimedia network company data. LSB embedding can also be applied to certain data areas - for example, embedding hidden message in RGB bitmap data values, or in JPEG image frequency coefficients. LSB embedding can also be used in a variety of data formats and types. Therefore, LSB embedding is one of the most important methods of steganography used today.

II. LITERATURE SURVEY

Rama Moortht et el [1] has mainly focused on the usage of the steganography to hide the data. Algorithm to perform cryptographic hash function. Data Embedding Phase and Authentication Phase and whole data is stored as an image in bank side , in which information about the customer is saved and hashing is done. Authentication will be done by comparing the hash values. The given methodology involves use of OTP (One Time Password) which creates security issues in the whole process.

Ramadhan J.Mstafa et el [2] has Discussed about different techniques of information hiding and Digital watermarking to mark all object in the same way. The concept of protection against detection and removal with watermarking and fingerprinting is discussed. The issue using that was described is Intensity of the colour affected.

Urang Awajionyi s et el [3] has proposed way of Secure ATM transaction using biometric fingerprint by Replacing the use of pin and bank credit card. The Precision of authentication was improved as identical matches are almost impossible. But this methodology is Prone to fingerprint spoofing and false detection of fingerprint. And require hardware upgradation.

Pavan S et el [4] has proposed concept of Concept of multifactor authentication was discussed and Authentication layer using IMEI number was introduced, and it was mentioned that by Using IMEI number and multifactor authentication security was improved but the feasibility of the proposed solution was very low.

Frimpong Twum et el [5] has suggested Three tier design structure. Application evaluation system based on False Rejection Rate(FAL), False Acceptance Rate (FAR), Average Matching Time (AMT) was discussed. The concept to evaluate the system using different scale was introduced but The solution is not feasible as it require hardware upgradation.

Indrajit Das et el [6] has introduced Finger vein authentication method as well as Light-weight cryptography and steganography (MSB-LSB) algorithm has been proposed and The average recognition accuracy is 98.75% and 97.2% with execution time 0.168 s but the The vein authentication method is relatively complicated.

Ketan Ramaneti et el [7] has generated stego images using Generative Adversarial Networks (GANs) and Extractor model was improved with high accuracy. The accuracy of 92.34% achieved by the extractor model but Processing time is relatively slow.

Abdul Alif et el [8] introduced Steganography with data mapping and Method to eliminate steganalysis attacks. So, the proposed methodology Able to achieve 3.48% larger embedding capacity. But it was Not able to achieve adaptable mapping between the cover and secret data bits.

Oleg Evsutin et el [9] gave Classification of methods for data hiding in digital images and Reverse engineering (Steganalysis). A detailed classification of steganographic algorithms but the Embedding efficiency is low.

Sabyasachi Pramanik et el [10] Approaches for information hiding using both cryptography & steganography is proposed keeping in mind two considerations - size of the encrypted object and degree of security. It Cover image with hidden data in encrypted using cryptography, but Execution is relatively high.

➢ *Design Methodology*

The proposed methodology involves the use of Steganography and Image Processing. The main aim of this research is to develop and introduce a new way of ATM transaction using Steganography technique where each time a dynamic ATM pin is created and encrypted inside an image which will be accessed by the user through their mobile by scanning a QR code during the transaction. The steganographic image will be decrypted only using the user's profile password. And Image Processing will be used to identify the person and send alert notification to customer's original and alternate number if more than 3 wrong attempt is made to decrypt the image during the live transaction.

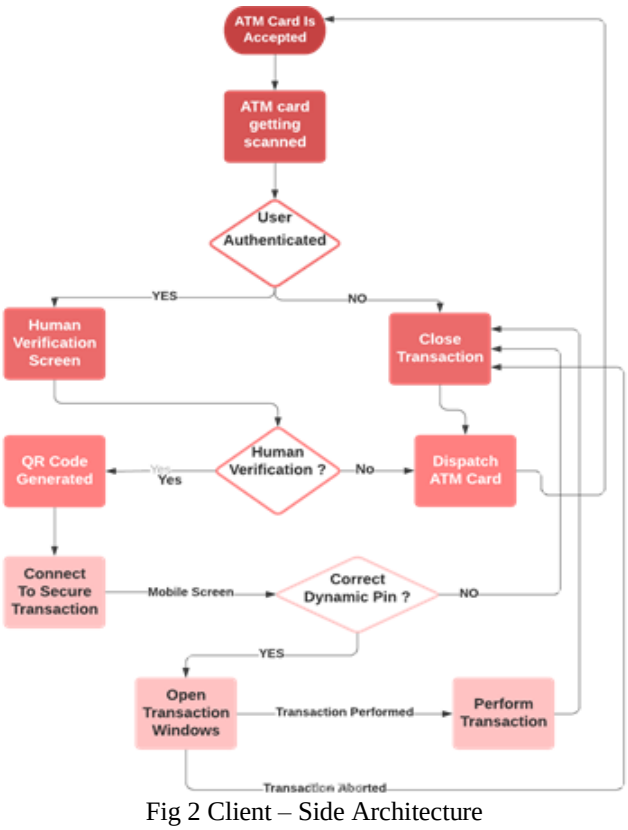

Fig 2 Client – Side Architecture

In the above Fig. 2 The client or the end user must Swipe the card in the ATM machine and the machine will check the authenticity of the card and this functionality will not be affected or will not be changed in the proposed system. Then the ATM card will be scanned, and the user authentication will appear to check the authenticity of the user. Here the user must enter password, it is just basically a four-digit user pin that the user must input in order to proceed. If the user will give wrong password, then the transaction will be closed. If the verification is successful, then a QR code will be generated and in the mobile phone the user has to install the application and again there will be option for sign up and Sign In , if the user is using this service for first time he needs to enter in the Sign Up section and has to register itself for making use of service and he/she is resisted then they have to tap on Sign In button in order to access the dashboard of the profile. Once after filling the credential the user can slide the Log In button in order to access the dashboard there, the card that are connected to the account will be displayed and option like check details of the account , statement , balance check will be there and in centre there is a button stating Tap To Transect that will be used to scan the QR code that was generated from the server side and is transmitted through secure server to perform the transaction. So once the user scans the QR code he/she will get a prompt to decrypt the dynamic PIN and that PIN has to be entered by user in the ATM to proceed with the transaction.

If the Dynamic PIN is incorrect then the transaction will be closed if the PIN is correct then transection window will be opened and the User can perform the transection or user can Abort the transection in between. In both the cases in the end the transaction will be cancelled and when each time the transaction is cancelled the user will get a chance to apply for a new Debit or Credit card. This are the required steps for performing the ATM transection and the functionality of the client-side architecture. The proposed work aims to enhance the security of ATM transection system as well as reduce the risk of external threads while performing the ATM transactions.

In the above Fig. 3 Firstly the server will check the connection, if the connection is not established then the transaction will be closed automatically and if the connection is successful then a four-digit PIN will be generated randomly, if the system is able to generate four digit PIN then from a pool of image a random photo will picked otherwise system will try to generate a four digit PIN again. If the Random photo is picked then the steganography is performed , it is performed using MSB method. After the encrypted image is created then the it is transferred to the client side using a secure server and then user profile password is checked if the profile password is incorrect then the user will get two more attempts , even after two more attempts if the user password is incorrect then Threat alert system will be activated and the image of the transaction will be captured and alert message and mail will be sent to the user registered Email and Contact number and transection will be closed. If the Password is correct then then the decoding of the encrypted image will be done and both passwords will be cross checked if they both are same then the access will be granted and then the transaction will proceed.

Fig 3 Server – Side Architecture

The server side and the client side of the proposed system is inter-connected with each other and help to reduce the risk in making transections using ATM. The Server side plays a major role and we have used the method of encryption where the specialised algorithms are used where we are manipulating the most significant bit of the structure and the pool of image will also be updated with new images.

For implementation we have prepared ten modules that are:

- *Login with OTP:*

The Login with OTP module enables us to Login using registered mobile number, user just has to enter the registered mobile number and request for OTP after entering the OTP the User has to slide the button and authentication will be done if the OTP entered by the user is correct then the user will send to the dashboard otherwise Error message will be displayed and User has to enter the mobile number again.

- *Transact Module:*

The Transect module gives us the option for scanning the image and get the Dynamic password that was generated and then encrypted and sent over the secured server. Firstly, the user needs to login then click on transect

ISSN No:-2456-2165

icon then scan the QR code that is generated and displayed on the ATM screen.

- *Decrypter Module:*

The Decrypter modules works for decryption of the encrypted image , here the image and the information or the four digit PIN are separated , in order to perform this operation user needs to scan the QR Code that is generated and click on the decrypt option on the Pop – up generated.

- *Scan Card Module:*

The Scan card modules is implemented to check the authenticity of the Card that is inserted into the ATM . This particular module reads the information that is present in card chip that is already embedded in the card then use that information to cross check the authenticity of the card by matching the information. If the card that is inserted is found illegal then the transaction will be closed automatically.

- *Banking Option Module:*

In this module the user gets option to select various option in order to get information regarding the account. In this module user gets options of account details, statement , Current account balance , change account setting and option for transferring money and this is dashboard for performing , it can be accessed by just logging into the account.

- *Encrypter with Dynamic PIN:*

In this module , the server is responsible for checking of established connection if the connection is not established then the transaction will be closed. If the transaction is established then the system will generate four digit Pin and once the image is generated an image will be picked randomly from pool of image and encryption will be done and that encrypted image will be transferred to the ATM.

- *PIN Verify Module:*

In this module PIN verification is done , the dynamic PIN will be matched with the generated PIN , here if the authentication is failed then the transaction will be closed and user will allowed to enter PIN three times , if the user enters three more consecutive wrong PINs then the transaction will be closed and threat alert system will be activated. In this module the PIN verification is described it works same as OTP and it makes process fast.

- *Transection Close Module:*

The Transection close module will allow close the transaction if authentication issues are there. The system will automatically close if it detects any suspicious activity and in few stages it will also trigger threat alert.

III. RESULT

To analyse the result of the current work, let's first go to the study of the previous work. In Chetana et al [3] the signature image is scanned by the application and then fed to pre-processing, where the intensity of the image is increased and then undergoes the generation of actions. The actions are stacked for authentication. Where, as during this work, the image is generated immediately after the data embedding process and a generation of actions is carried out, represents the comparison. Transactions suggested Fadi Aloul et al. within the server. So, the key needs to be sent back to the server for verification and it is not said to have immediate verification. In the later stages of the transaction, the user is verified. Therefore, in this job, the key is specified as follows: It is generated on the device on which the transaction is taking place, and only the key is sent via SMS to the mobile phone to the specific registered number of the user who is performing the transaction, so that the authentication carried out in the input phase, faster and more efficiently.

To overcome this issues several solutions were given in the form of biometric solution as well as two factor authentication but they don't seems to be practical as the tends to increase time for each transection as well as those methods comes with increase cost of deployment and these methods also needs hardware upgrade. To overcome these issues, we have proposed a new method of performing ATM transactions. So, in this method we have used steganographic and visual cryptography technique approach on image processing with the help of mobile phone. The proposed system uses live ATM transaction with steganography to generate dynamic pin for each new ATM transaction performed. The concept of 4-digit static pin is eliminated with the 4-digit dynamic pin. Whenever a transaction is performed a random 4-digit pin will be generated by the server and it will be steganographic with an image which will be visible to user on his mobile screen. The user needs to type their profile password and the encrypted pin in the image will be visible and can be used to perform transection. In case of 3 wrong attempts the image of the person who is performing the transaction will be captured and the alert system will send alert messages to user's main and alternate mobile number. the direct use of encryption is eliminated because the encrypted messages will trigger the hackers.

That some important information is being transferred via the respective channel. The crucial prerequisite in these days is to get rid of various forms of attacks.

So this Method is unique in obtaining a solution for Authentication of a customer for Bank as well as for ATM transactions.

ISSN No:-2456-2165

Fig 4 Depiction of Login

The Fig. 4 depicts the option for login of the user if the user has Account number and password that was provided by the bank then user can directly Login other wise user can login with the option Login with OTP.

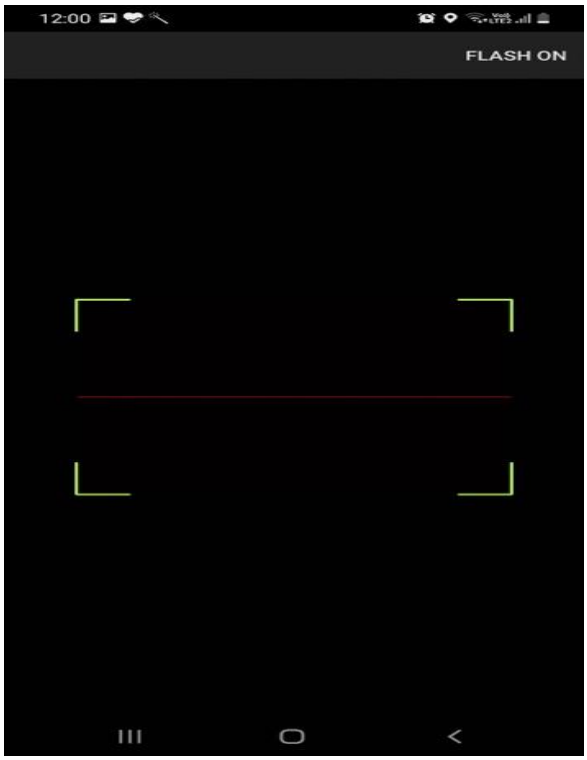

Fig 5 Depiction of Decryption of Key

The given fig. 5 shows the image of scanner where user can scan the encrypted image and then user will get pop up of decryption of the code.

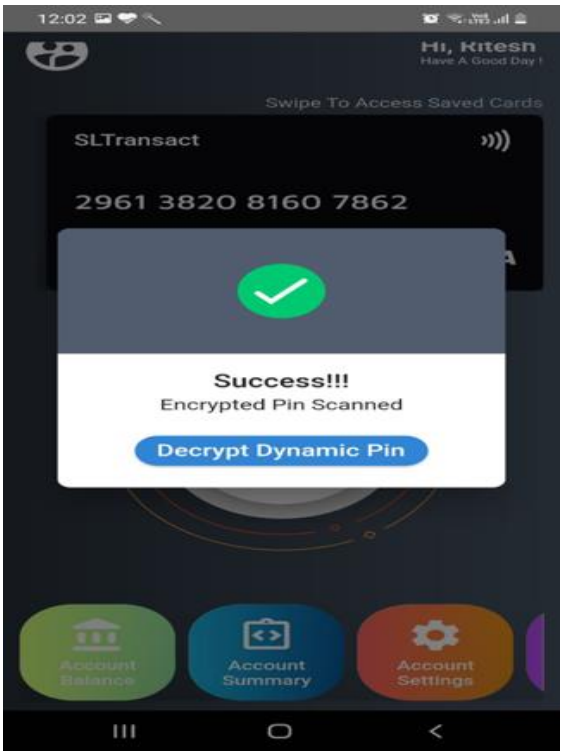

Fig 6 Depiction of Decryption of Key

The above given fig.6 shows the option for decryption of the encrypted image so that the user can enter the four digit dynamic Pin in the ATM machine , so that he/she can continue with the transaction. If the user enters wrong password he/she has three more attempts if user is failed in that then the transaction will be closed and alert threat system will be activated.

IV. CONCLUSION

The paper method to finish the traditional or the antique approaches of transaction utilized in ATM ought to get replaced via way of means of the Steganography approach wherein the transaction technique turns into extra secured and dependable. All the customers want to hold their very own cellular telephones to have their transaction to finish and affirm their identification. It is primarily based totally at the traits of scanning the picture withinside the ATM thru the telecellsmartphone and getting the dynamic pin from it and it'll deliver get entry to the technique of transaction and it'll assist it grow to be extra secured. Steganography lets in the recognition of a personal thru quantifiable physiological traits that affirm the identification of a man or woman. AES 256 encryption presents stable protection functions required for the system. Steganography mechanism presents little or no clue to centre guy assaults. With the deliver low price-green biometric scanners, this method is positive to deliver a alternative enjoy to the customers, who can sense the benefit of use and on the identical time happy as no compromise has been made to the protection factor of the system. Due to an enlargement in globalization, the ordinary man or woman's existence has been compromised via way of means of the increasing grievous occasions of

assaults of man or woman statistics and withinside the case of monetary transaction and banking-associated duties in coins device machines (ATMs). PIN and Password are maximum not unusual place manner of getting access to ATMs for monetary transaction however they may be cast and consequently are subjected to assault including phishing, spoofing etc. In order to triumph over such assaults better protection is needed. Subsequently the human physiological and behavioural traits, as an example iris, voice, finger print, face palm and so forth are being applied to offer higher protection arrangements. In any case, all of them may be correctly deceived and replicated at one stage and a advanced association is needed for the safety requirements which might be price effective and dependable too. Hence, the mixed method (device getting to know and picture processing) of finger vein authentication approach is hired and for finger vein picture switch variable MSB–LSB steganography and light-weight weight cryptography is proposed on this paper. The vein authentication approach is exceedingly complicated, so it may be higher to apply it for a few unique applications. For finger-vein authentication system, the test indicates that during proposed class manner (one-versus- one and one-versus-all) the common reputation accuracy is 98.75% and 97.92% and the execution time is 0.168 s and 0.187 s respectively. One comparative look at is finished amongst five algorithms which includes ANFIS, Global Matching and SVM, MLP, SVM and CNN. Adaptive neuro-fuzzy inference system (ANFIS) and convolutional neural network (CNN), the 2 algorithms have higher class accuracy than proposed method i.e., with 99% and 99.38 accuracy respectively. However, the execution time of 4. five s is needed for ANFIS which is relatively extra than proposed manner and CNN aren't giving green end result for low exceptional finger vein images, while the proposed manner has no such difficulty. Thus, the proposed method is pleasant in regards to class accuracy while seemed in a different way in connection with ANFIS and CNN and moreover have effective if there ought to be an incidence of time of execution, noise sensitivity and higher for non-best finger vein cases. Another difficulty that's to be taken into consideration is that the method via way of means of which this biometric picture (finger vein) is frequently transferred safely. And the variable MSB–LSB set of rules is higher than easy LSB set of rules as it calls for a smaller wide variety of pixels for embedding and feature higher randomness, protection etc.

Generated Shares if revealed also to any third party, through hacking of database or stealing of the card, does not reveal any information regarding the customer has only a hash value is stored, particular system is considered to authenticate a user only in a bank. The PIN generated with the help of a image and the data hidden, will be sent to the registered Mobile Number of that particular customer as a message only. As to this method, the PIN generated is from ATM machine itself, therefore no need to wait to ATM server to validate the PIN entered. Thus, we can achieve Dynamic Key and validation is done at entry level rather than later stages of the ATM transaction.

The process could also be considered for the network banking facility to provide two levels of user authentication. From now on, authentication takes place with two-step user names and passwords.

REFERENCES

[1]. Rama Moorthy H et al., “Steganographic And Visual Cryptographic Approach For Authentication Of Bank Users Using ATM Cards ”, International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 5, May - 2013. [Online].Available:https://www.ijert.org/research/steganographic-and-visual- cryptographic-approach-forauthentication-of-bank-users-using-atm-cards-IJERTV2IS50805.pdf

[2]. Ramadhan Mstafa et al., “Information Hiding in Images Using Steganography Techniques ”, I2013 ASEE Northeast SectionConferenceMarch1416,2013[Online].Available:https://www.researchgate.net/publication/259893801_Information_Hiding_in_Images_Using_Steganography_Techniques

[3]. URANG Awajionyi S et al., “Securing Automated Teller Machine (ATM) Transaction Using Biometric Fingerprint ”,American Journal of Engineering Research(AJER) Volume9,Issue9,pp3643[Online].Available:http://www.ajer.org/papers/Vol-9-issue-9/F09093643.pdf

[4]. Ketan Ramaneti et al., “Image Steganography Using GANs”,ICIS2021:ComputerStegnographyusingGAN’spp1918224June2021.[Online].Available:https://link.springer.com/chapter/10.1007%2F978-3-030-79474- 3_12

[5]. Frimpong Twum et al., “Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication ”, International Journal of Science and EngineeringApplicationsVolume 5 Issue 3, 2016, ISSN-23197560(Online) [Online]. Available:https://www.researchgate.net/publication/301536500_Improving_Security_Levels_In_Automatic_Teller_Machines_ATM_Using_Multifactor_Authenticati on

[6]. Indrajit Das et al., Design and implementation of secure ATM system using machine learning and crypto–stego methodology ”, pringer Nature Switzerland AG 2019 SNAppliedSciences(2019)1:976[Online].Available: https://doi.org/10.1007/s42452-019-0988-0

[7]. Rama Moorthy H et al., “Steganographic And Visual Cryptographic Approach For Authentication Of Bank Users Using ATM Cards ”, International Journal of Engineering Research& Technology (IJERT)Vol.2Issue5,May2013.[Online].Available:https://www.ijert.org/research/steganographic-and-visual-cryptographic-approach-for-authentication-of-bank-users-using-atm-cards-IJERTV2IS50805.pdf

[8]. Abdul Alif Zakaria et al., "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution ", MPDI , Applied Science *Appl.Sci.*2018,*8*,2199[Online]. Available:https:https://www.mdpi.com/2076-3417/8/11/2199

[9]. Oleg Evsutin et al., "Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions ", IEEE Access *Volume: 8, Septempber-2020*[Online].Available :https://ieeexplore.ieee.org/document/9187785

[10]. Sabyasachi Pramanik et al., "Signature Image Hiding in Color Image using Steganography and Cryptography based on Digital Signature Concepts", 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) *Volume 4.* March 2020 [Online].Available:https ://ieeexplore.ieee.org/document/9074957