iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 5 **Issue:** III **Month of publication:** March 2017

**DOI:** http://doi.org/10.22214/ijraset.2017.3106

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# A Hybrid Data Hiding Approach for Securing Online Transactions

Ms. Prachi D. Rathod[1], Mrs. Smita R. Kapse[2]
[1]M.Tech Student, [2]Assistant Professor, Department of Computer Science and Engineering
Yeshwantrao Chavan College of Engineering, Nagpur, India

***Abstract:*** ***Online Banking is an arrangement of administrations given by a gathering of organized bank offices. Bank clients may get to their assets and perform other basic exchanges from any of the part branch workplaces. The real issue in centre keeping money is the realness of the client. Authentication login plays noteworthy roles in this day and age. Because of unavoidable hacking of the databases, it is dependably very hard to confide in the data. The venture work means to tackle the issue of legitimacy. In this paper, we are proposing a system using picture preparing, Steganography and visual cryptography, and after that separating it into shares. In this venture the Transaction Password is taken as a contribution from the client who needs to get implanted in the picture document. The picture record will be of the augmentations .jpg. The message process is figured utilizing the RSA algorithm and this is affixed with the message. The affixed encoded message is inserted in the picture utilizing the minimum huge piece calculation. The encoded picture is then divided into two shares utilizing Shamir's Secret Sharing Scheme. At the point when two shares are made, one is put away in the Bank database and the other is kept by the client or sends to E-Locker server. E-Locker Server is also secured by a dynamic character location based mechanism which is a new concept introduced as a contribution in this paper. The client needs to introduce the share amid the greater part of his exchanges. This impart is stacked to the primary share to get the first Transaction key. The Correlation strategy is utilized to take the choice on acknowledgment or dismissal of the yield and verify the client.***
***Keywords: Information security, Steganography, Visual Cryptography, Online Banking.***

## I. INTRODUCTION

Today, most applications are just as secure as their hidden framework. Since the plan and innovation of middleware has enhanced consistently, their identification is a troublesome issue. Subsequently, it is almost difficult to make sure whether a computer that is associated with the web can be viewed as reliable and secure or not. The question is the way to deal with applications that require an abnormal state of security, for example, center managing an account and web keeping money. In a center managing an account framework, there is a shot of experiencing fashioned mark for exchange. Also, in the net managing an account framework, the secret key of client might be hacked and abused. In this manner security is still a test in these applications. Here, we propose a system to secure the client data and to keep the conceivable fabrication of marks and secret word hacking.

Steganography is the craftsmanship and exploration of composing shrouded messages in a manner that nobody, aside from the sender what's more, expected beneficiary, associates the presence with the message, a type of security through lack of definition. The word steganography is of Greek root and means disguised written work. For the most part, messages will have all the earmarks of being something else: pictures, articles, shopping records, or some other cover content and, traditionally, the shrouded message might be in undetectable ink between the obvious lines of a private letter. The benefit of Steganography, over cryptography alone, is that messages don't pull in consideration regarding themselves. Consequently, while cryptography secures the substance of a message, steganography can be said to ensure both messages and conveying parties. Steganography incorporates the covering of data inside computer documents.

In advanced steganography, electronic correspondences may incorporate steganographic coding within a vehicle layer, for example, a report record, picture document, program or convention. Media documents are perfect for steganographic transmission on account of their vast size. Steganography can be seen as much the same as cryptography. Both have been utilized all through written history as intends to secure data. Now and again these two advances appear to focalize while the targets of the two vary.

Cryptographic systems "scramble" messages so if captured, the messages can't be caught on. Steganography, in a pith, "disguises" a message to shroud its reality and make it appear to be "undetectable" accordingly covering the way that a message is being sent by and large.

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A scrambled message may draw doubt while imperceptible messages won't Authentication of steganographic data includes confirming that the message sent by the sender is the thing that got by the recipient and is not controlled by the interloper.

Visual Cryptography (VC) is a strategy for encoding a mystery picture into shares with the end goal that stacking an adequate number of shares uncovers the mystery picture. Steganographic techniques consider human vision affectability as a basic element so that the very presence of the mystery bits couldn't be uncovered by any outsider. The idea of picture preparing, an enhanced Steganography and visual cryptography is utilized as a part of this paper. Picture handling is a procedure of preparing an information picture and to get the yield as either enhanced type of a similar picture and additionally qualities of the information picture. Visual Cryptography (VC) is a strategy for scrambling a mystery picture into shares with the end goal that joining an adequate number of shares uncovers the mystery picture amid the login.

Naor and Shamir [2] presented a straightforward however totally secure way that permits mystery sharing with no cryptographic calculation, named as Visual Cryptography Scheme (VCS). Essentially, Visual Cryptography Scheme is an encryption strategy that utilizations combinatorial strategies to encode mystery composed materials. The idea is to combine the composed material into a picture and encode this picture into n shadow pictures.

A segment based visual cryptography recommended by Borchert [6] can be utilized just to scramble the messages containing images, particularly numbers like ledger number, sum and so on., Steganography is the specialty of hiding the presence of data inside apparently harmless bearers. Steganography is the act of concealing private or touchy data inside something that has all the earmarks of being nothing out of the standard thing. Steganography is frequently mistaken for cryptology in light of the fact that the two are comparable in the way that they both are utilized to secure essential data. The distinction between the two is that Steganography includes concealing data so it creates the impression that no data is covered up by any means. On the off chance that a man or a person sees the question that the data is covered up within he or she will have no clue that there is any concealed data, consequently the individual won't endeavor to decode the data. Cryptography and Steganography has been for quite a while. Prior a message was ciper utilizing cryptography and sent to beneficiary, despite the fact that it was secure approach yet it was obvious message amid. To make it undetectable message next they connected steganographic technique. Truth be told, steganography can be helpful when the utilization of cryptography is taboo: where cryptography and solid encryption are banned.

Steganography can maintain a strategic distance from such approaches to pass message secretively. Be that as it may, steganography and cryptography contrast in the way they are assessed: Steganography comes up short when the "foe" can get to the substance of the figure message, while cryptography falls flat when the "adversary" recognizes that there is a mystery message exhibit in the steganographic medium. The orders that review systems for decoding figure messages and distinguishing shroud messages are called cryptanalysis and steganalysis. The previous indicates the arrangement of strategies for acquiring the significance of scrambled data, while the last is the specialty of finding incognito messages.

Naor and Shamir [2] presented Visual Cryptography in 1994. The essential model of Visual Cryptography expects that the mystery message comprises of high contrast pixels. Every mystery pixel is either partitioned into two subpixels or four subpixels. These subpixels frame the shares for the mystery message. There are distinctive or comparative sub pixel designs in light of the mystery pixel as per Figure 1.

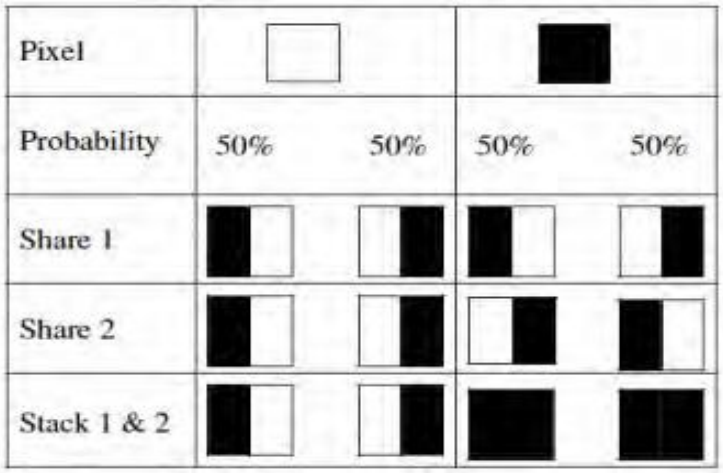



Figure 1: 2 out of 2 scheme using 2 subpixels per original pixel.

The inferred structure can be described in the form of m×n Boolean matrix S = [sij] where sij=1 iff the jth subpixel of the ith share is black. These sub pixels are then printed on transparent sheets so that overlapping the transparent sheets reveals the secret message. The gray level value of this pair of shares is equal to the Hamming Weight H(V) of the "or" ed m-vector V. The graylevel is visualized as black if H (V) ≥ d and white if H(V)≤ d-α.m for some fixed threshold 1≤d≤m and relative difference .

*A. Various Visual Secret Sharing Schemes Existing are*

*1)* (n, n) Visual Secret Sharing Scheme

*2)* (k, n) Visual Secret Sharing Sche

*3)* (n, n) Visual Secret Sharing Scheme is where the secret is separated into a total of n shares and all the n shares are overlapped to get visually read the secret message.

(k, n) Visual Secret Sharing Scheme is where the secret is separated into n shares and any k or more of these shares when overlapped reveals the secret.

(k, n) Visual Secret Sharing Scheme consists of two collections of n×m Boolean matrices C0 and C1. At the point when a white pixel is shared, any of the lattices out of the accumulation in C0 is picked. What's more, when a dark pixel is craved to be shared, anybody framework out of all in the accumulation in C1 is considered. The accompanying conditions are to be fulfilled to uncover the mystery in a (k, n) Visual Scheme utilizing the above frameworks.

*4)* For ant S in C0, the "or" V of any k of the n rows satisfies H(V)≥ d.

*5)* For any subset {i1, i2, ……,iq} of {1, 2,….. , n} with q< k, the two collections of q×m matrices Dt for t obtained by restricting each n×m matrix in Ct (where t={0, 1}) to rows i1, i2, …… ,ir are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The third condition implies that if not as much as k shares are examined, it is practically difficult to increase any learning about the mystery pixel shared being dark or white. The initial two conditions are to guarantee the differentiation and the third condition guarantees security. The parameters, m = the quantity of pixels in a share. Otherwise called the pixel development ought to be as little as conceivable to hold the determination of the first picture in a decoded picture.

α = the relative difference. This represents the loss in contrast and hence it must be as large as possible.

r = the size of the collections C0 and C1.

## II. RELATED WORK

A short study of the related work in the range of visual cryptography and its application in managing an account part is introduced in this area. In [1] a mechanism to provide an minimal information that is necessary for transaction during online shopping thereby preserving customer data privacy and preventing identity theft. The method uses a hybrid implementation of steganography and visual cryptography. Visual cryptography plans were freely presented by Shamir [2], [3] and Blakley [4], and their unique inspiration was to defend cryptographic keys from misfortune. These plans likewise have been broadly utilized in the development of a few sorts of cryptographic conventions [5] and subsequently, they have numerous applications in various territories, for example, get to control, opening a bank vault, opening a security store box, or notwithstanding propelling of rockets. A portion based visual cryptography recommended by Borchert [6] can be utilized just to encode the messages containing images, particularly numbers like ledger number, sum and so forth., the VCS proposed by Wei-Qi Yan et al., [7] can be connected just for printed content or picture. A recursive VC technique proposed by Monoth et al., [8] is computationally mind boggling as the encoded shares are further encoded into number of sub-shares recursively. Additionally a procedure proposed by Kim et al., [9] likewise experiences computational unpredictability, however it abstains from dithering of the pixels.

The greater part of the past research deal with VC concentrated on enhancing two parameters: pixel development and complexity [10], [11], [12]. In these cases all members who hold shares are thought to be straightforward, that is, they won't present false or fake shares amid the period of recuperating the mystery picture. Consequently, the picture appeared on the stacking of shares is considered as the genuine emit picture. Be that as it may, this may not be genuine dependably. In this way, a tricking counteractive action approaches are presented by Yan et al., [13], Horng et al., [14] and Hu et al., [15]. Be that as it may, it is seen in every one of these techniques, there is no office of confirmation testing. In this paper, we propose a VC technique in view of pixel networks and a strategy for confirmation.

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

## III. METHODOLOGY

Our project proposes a mechanism of processing a secret key of a user and then splitting it into shares. When two shares are created, one is stored in the Bank database and the other is kept by the user. The user has to use the share during all of his transactions. This share is stacked with the first share get the original secret key. The Correlation method is used to take the call on acceptance or rejection of the output and authenticate the customer.

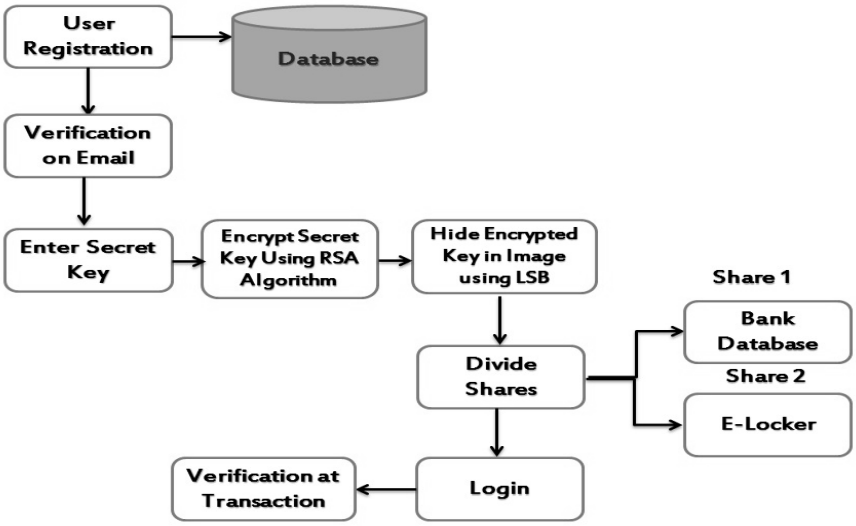



Figure 2: System Architecture

### A. *Algorithms*

1) *Least Significant Bit:* The minimum huge piece (as such, the eighth piece) of a few or the greater part of the bytes inside a picture is changed to a touch of the mystery message. Digital pictures are predominantly of two sorts (i) 24 bit pictures and (ii) 8 bit pictures. In 24 bit pictures we can insert three bits of data in every pixel, one in each LSB position of the three eight piece values. Expanding or diminishing the incentive by changing the LSB does not change the presence of the picture; much so the resultant stego picture looks practically same as the cover picture. In 8 bit pictures, one piece of data can be covered up.

The cover picture is appeared in Figure 3 and a shrouded message is appeared in Figure 3 a stego-picture is gotten by applying LSB calculation on both the cover and concealed pictures. The concealed picture is removed from the stego-picture by applying the switch process[1, 11]. On the off chance that the LSB of the pixel estimation of cover picture C(i,j) is equivalent to the message bit m of mystery back rub to be implanted, C(i,j) stay unaltered; if not, set the LSB of C(i, j) to m. The message inserting methodology is given beneath

$$S(i, j) = C(i, j) - 1, \text{ if } LSB(C(i, j)) = 1 \text{ and } m = 0$$
$$S(i. j) = C(i, j), \text{ if } LSB(C(i, j)) = m$$
$$S(i, j) = C(i, j) + 1, \text{ if } LSB(C(i, j)) = 0 \text{ and } m = 1$$

Where LSB(C (i, j)) remains for the LSB of cover picture C (i, j) and m is the following message bit to be implanted. S (i, j) is the stego picture as we definitely know every pixel is comprised of three bytes comprising of either a 1 or a 0.

For instance, assume one can conceal a message in three pixels of a picture (24-bit hues). Assume the first 3 pixels are:

(11101010 11101000 11001011)
(01100110 11001010 11101000)
(11001001 00100101 11101001)

A steganographic program could conceal the letter "J" which has a position 74 into ASCII character set and have a parallel portrayal "01001010", by changing the channel bits of pixels.

(11101010 11101001 11001010)
(01100110 11001011 11101000)
(11001001 00100100 11101001)

For this situation, just four bits should have been changed to embed the character successfully. The subsequent changes that are made to the minimum critical bits are too little to possibly be perceived by the human eye, so the message is successfully covered up.

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

The benefit of LSB implanting is its effortlessness and numerous strategies utilize these techniques. LSB installing additionally permits high perceptual straightforwardness.

The following figure 3 shows the mechanism of LSB technique:

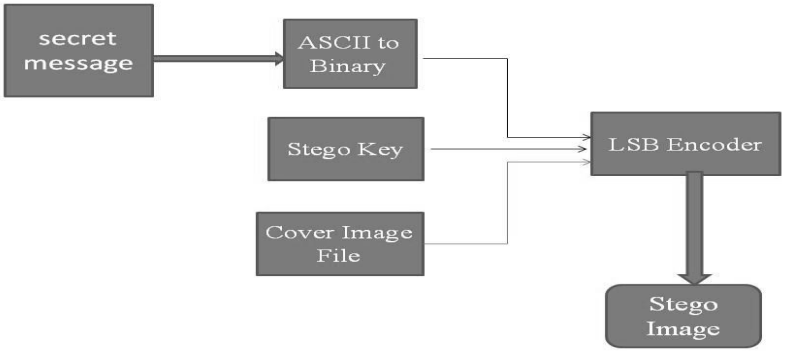



Figure 3: LSB Flowchart

*2) The Embedding Process is as Follows*: Inputs Cover image, stego-key and the text field

Output stego image

Procedure:

Step 1: Select the pixels of the cover image.

Step 2: Select the characters of the text file.

Step 3: Select the characters from the Stego key.

Step 4: Select first pixel and pick characters of the Stego key and place it in first component of pixel.

Step 5: Place some terminating character to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.

Step 6: Insert characters of text field in each first component of next pixels by replacing it.

Step 7: Repeat step 6 till all the characters has been embedded.

Step 8: Again place some terminating character to indicate end of data.

Step 9: Obtained stegno encoded image.

*3) The Extraction Process is as Follows:* Inputs Stego-image file, stego-key, Output Secret text message.

Procedure:

Step 1: Extract the pixels of the stego image.

Step 2: Now, start from first pixel and extract stego key characters from first component of the pixels. Follow Step3 up to terminating symbol, otherwise follow step 4.

Step 4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.

Step 5: If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.

Step 6: Extract secret message.

*B. RSA Algorithm*

RSA encrypts data through the following steps, which is divided into 3 segments

*1) Key Generation:*

*a)* Choose two unique prime numbers p and q.

*b)* Find n such that n = pq. N will be used as the modulus for the public as well as private keys.

*c)* Find the totient of n, $\phi(n)$

*d)* $\phi(n) = (p-1)(q-1)$.

*e)* Choose an e such that $1 < e < \phi(n)$, and such that e and $\phi(n)$ shares no divisors other than 1 (e and $\phi(n)$ are closely prime). e is considered as the public key exponent.

*f)* Find d (using modular arithmetic) which satisfies the congruence relation

$$de \equiv 1 \pmod{\phi(n)}.$$

In other words, select d such that de - 1 can be evenly divided by (p-1) (q-1), the totient, or $\phi(n)$.

This is often calculated using the Extended Euclidean Algorithm, since e and $\phi(n)$ are closely prime and d is to be the modular

multiplicative inverse of e. d is kept as the private key exponent.
The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n with the private exponent d, which is kept secret.

*C. Encryption*

*1)* A transmits public key (modulus n and exponent e) to B, keeping his/her private key secret.
*2)* When Person B wants to send the message "M" to Person A, he first converts M to an integer such that $0 < m < n$ by using agreed upon reversible protocol known as a padding scheme.
*3)* Person B calculates, with Person A's public key information, the ciphertext c corresponding to
*4)* $c \equiv me \pmod n$.
*5)* B now sends message "M" in ciphertext, or c, to A.

*D. Decryption*

A recovers m from c by using his/her private key exponent, d, by the computation

$$m \equiv cd \pmod n.$$

Given m, A can recover the original message "M" by reversing the padding scheme.
This procedure works since

$$c \equiv me \pmod n,$$
$$cd \equiv (me)d \pmod n,$$
$$cd \equiv mde \pmod n.$$

By the symmetry property of mods we have that

$$mde \equiv mde \pmod n.$$

Since $de = 1 + k\,\phi(n)$, we can write

$$mde \equiv m1 + k\phi(n) \pmod n,$$
$$mde \equiv m(mk)\phi(n) \pmod n,$$
$$mde \equiv m \pmod n.$$

From Euler's Theorem and the Remainder Theorem, we can show that this is true for all m and the original message

$cd \equiv m \pmod n$, is obtained.

*E. Shamir's Secret Sharing*

In this scheme the initial two speaks to the aggregate number of shares made for the first picture and the second two speaks to the base number of shares required to decode the picture. The VCS model is subject to the premise grids. Premise is the arrangement of directly free vectors. The whole (2, 2) VCS model can be depicted by two premise lattices: one for dark pixel and one for white pixel. The premise lattices of (2, 2) VCS model are:

$B_0 =$

| | |
|---|---|
| 1 | 0 |
| 1 | 0 |

And $B_1 =$

| | |
|---|---|
| 1 | 0 |
| 0 | 1 |

Here, component 1 implies the nearness of a dark pixel in the share picture produced from this lattice and component 0 implies the nearness of white pixel. Thus we could reason that, Visual Cryptography conspire spoke to in PC utilizing n x m Basis networks. Premise grids are parallel n x m used to encode every pixel in the mystery picture, where n is the quantity of members in the plan and m is the pixel extension.
The following algorithm is used to implement a VCS using basis matrices:

```
for each pixel p in S:
{
if(p is black)
   Let R = a random permutation of the columns of B1
```

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

```
    Else
       Let R = a random permutation of the columns of B0
    for each participant i (1 <= i <= n):
    {
    The position on participant i's share that corresponds to p is expanded into m pixels where each of these pixels
    j (1 <= j <= m) is black
    if Ri,j = 1
    and white
     if Ri,j = 0
    }
}
```

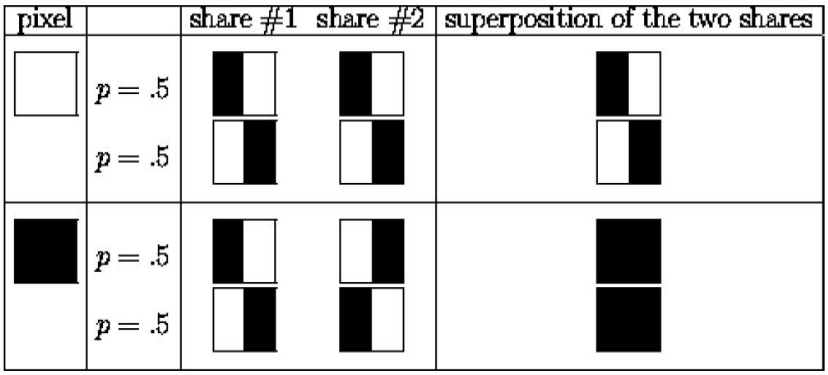



Figure 4: 2X2 Shamir Secret Sharing Model

In the event that the pixel to be scrambled is white, one of the two sections under white pixel is chosen (fig 4). On the off chance that the pixel to be scrambled is dark, one of the two sections under the dark pixel is chosen (fig 4). Subsequently, we see that for each situation choice is performed arbitrarily and every section has half likelihood to be picked. Along these lines, if the pixel to be encoded was white, it yields one dark and one white pixel and if the pixel was dark it yields two dark subpixels. This demonstrates the loss of difference.

## IV. MODULE IMPLEMENTATION

### *A. Homepage*

This is the Homepage of any banking website in which we have to login. In Home page various options are provide like login, new user, forget password, e-mail verification. If we already have an account in the bank, then using our login id and password we can login. During login if the customer forget his password then by the forget password option customer reset his password. And after getting the new password customer will login to the bank site and perform his transactions. By using the new user option you create your account in the bank site. If you are new user to the bank then you have to go through the registration process. In registration process you have to fill registration form in which you have to enter your name, surname, contact number this basic information and valid Email id and also set your password from this password the customer perform their transactions. After the registration process the email id verification performs. In customer mail account a verification code will receive and this code is receive into the email verification box if the customer enter a valid code then his registration done successfully. And now the customer is ready to perform his transaction.

### *B. User Registration*

If you are new user to the bank then you have to go through the registration process. In registration process you have to fill registration form in which you have to enter your basic information like your name, surname, contact number, and valid Email id and also your password from this password the customer perform their transactions. After the registration process the email id verification performs. In customer mail account a verification code will receive and this code is enter into the email verification box if the customer enter a valid code then his registration done successfully. And now the customer is ready to perform his transaction.

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

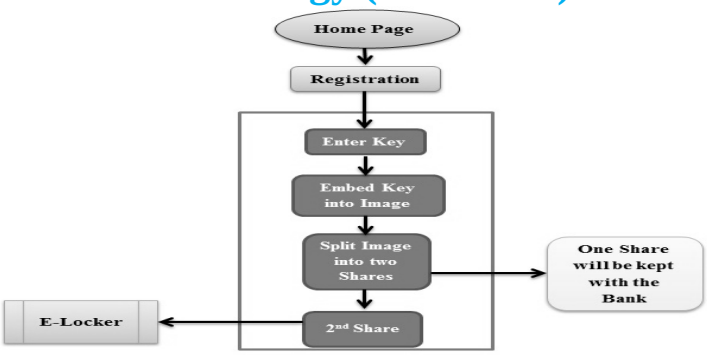



Figure 5: User registration process

*C. Email Verification*

A verification code will send to customer email id. This valid code is enter in the email verification box if the code is correct the registration done successfully. After successful registration you get your login id and password on your Email account. Using that Id and password we can login into the bank website. This login id and password are the permanent for your all the transactions process.

*D. Select Image and Generate Secret Key*

After successfully registration user have to select a image as per his choice whatever he want. Then user should upload the image then after he has to enter a secret key. this secret key is hide behind the image which user was select. Encrypted Secret Key Should is embedded with a selected image. This Image should be divided into two shares. One share should be downloadable and this downloadable image send to E-Locker and other should be stored into Bank Database.

*E. E-Locker*

This is bank side picture server, in which we can store our picture share. This E-Locker is secured by a new authentication framework where user needs to use location of the characters as a password. By utilizing straight forward Id and Password we can login into picture server. at that point this picture separate client ought to enter substantial email id then picture server approached the mystery address for e.g. what is your name according to your decision client ought to be set the question. At that point client see the character framework then enter your set the mystery address in the advanced arrangement. At that point client ought to back to login then open the administrator login frame.

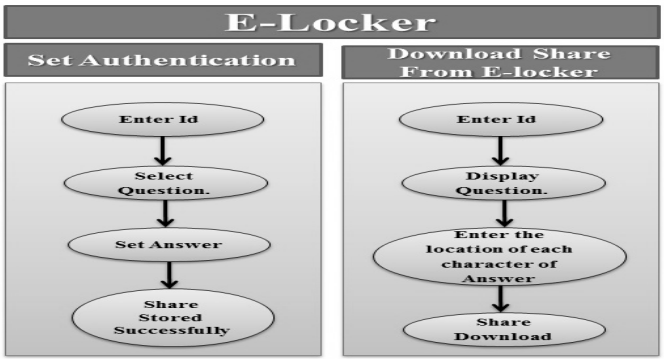



Figure 6: E-Locker Process

*F. User Login*

After effectively picture disjoin enrollment then back to login open the administrator login page. It is the client login in which after login we get the saving money account subtle elements. Yet, at the season of exchange we need to enter our share. This impart is converge to bank database share. Our mystery Key ought to be recovered and regarded as Transaction key.

After this procedure client ought to enter email id and secret word this id and watchword client could be used in the enlistment

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

procedure then login this id and secret key. After effectively administrator login check the record subtle elements .account confirmation handle we can pick the share picture peruse and transfer this site then check your bank points of interest. At that point after open the record subtle elements page then client ought to play out the exchange procedure.


Figure 7: User Login Process

## V. RESULTS AND DISCUSSIONS

In the proposed solution, information submitted by the customer is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a new Cryptographic Password System generated by the combined application of steganography and visual cryptography. The information received by the bank will be in the form of a Blur image i.e., the second share of visual cryptographic key. Transaction Key required for authentication in connection to the bank is encoded inside a cover image using the text based steganography method as mentioned. but it will only authenticate when the users share will be merged with the banks share. The information will only validate receipt of payment from authentic customer. Upon receiving customer authentication password, bank matches it with its own database and after verifying legitimate customer, transfers fund from the customer account to the submitted merchant account.

For the security of the users share a new key storage mechanism E-Locker. E-Locker Server is also secured by a dynamic character location based mechanism where user will have to remember the password but while login user will have to enter the location of the characters from the matrix which will be displayed.

Proposed method reduces the user information sent to the bank during transaction. So in case of a breach in merchant's database, customer doesn't get affected. It also prevents unlawful use of customer information at merchant's side. With our method the chance of Tradition Password attacks on web application like Brute Force, Spyware, and Phishing etc. is reduced significantly.

Attacks on online banking today depend on beguiling the client to take login information and substantial TANs. Two surely understood cases for those assaults are Phishing, Cross-site scripting and key logger/Trojan steeds can likewise be utilized to take login data.

A technique to assault signature based web based saving money strategies is to control the utilized programming as it were, that right exchanges are appeared on the screen and faked exchanges are marked out of sight. Call parodying is a system where by the fraudster fakes the telephone number on guest ID to give the feeling that you are being reached by a veritable Bank's number.

Our proposed mechanism basically counters almost all the possible Technical attacks [16] [17] [18]. The main reason for this is the hybrid approach of Steganography & Visual Cryptography. We developed a transaction key which will only reveal the original secret key when the other part of key will be superimposed on the later part.

Following are our observation on traditional attack on online banking and its effects on existing system & Proposed System:

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Table 1: Effects of attacks on online banking

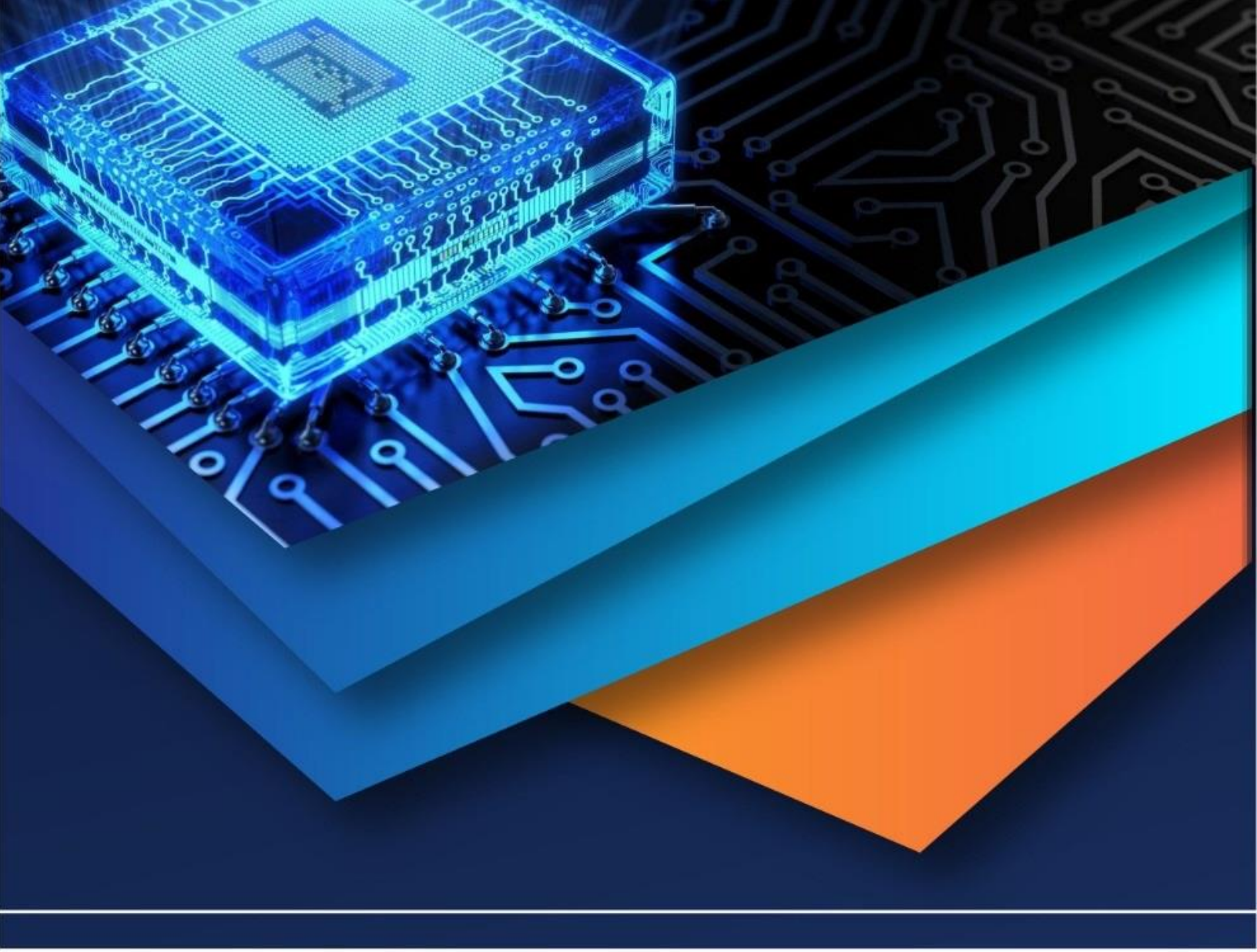
| Attacks | Existing System | Proposed System |
|---|---|---|
| Phishing | Easily Possible Fake page can be easily develops to manipulate the user. | Not Possible as the User share has to be downloaded from E-Locker locked on the Banks side. Fake will not have access to the original server. |
| Key logger/Spyware | Possible as Existing system rely on text based password. | Not Possible as we are relying on the share of image and not typing any form of text. |
| Cross Site Scripting | Possible as the data can be manipulated to be redirected on the different server. | Less Chances as every time we are relying on the same password but each time before using it we have to get it from E-Locker. |
| Spoofing | Possible as the Phone Call or message can be intercepted by Sim cloning or deploying a Trojan in cell phone to hijack OTP. | Less Chance as we are not relying on third party mechanism or device to get OTP but we have created a mechanism where user will enter new password every time though his/her password remains same. |

## VI. CONCLUSIONS

In this paper, an authentication mechanism for online banking is proposed by a hybrid text based steganography and visual cryptography that provides user data privacy and prevents unethical attacks. The method is concerned only with prevention of identity theft and customer data security. The traditional cyber attacks are infeasible on our system. We tried to maintain the efficiency of the system though it is takes a bit of more time but it is a simple fundamental that more the security more will be time to process. We introduce E-Locker which is secured with a dynamic character location based mechanism. Currently it is integrated with the banks server; in future we can implement it as an autonomous system for securing the transaction key. As we applied this approach for banking application, the proposed method can also be applied for any E-Commerce application with focus area on payment during online shopping as well as physical banking.

## REFERENCES

[1] S. Roy, P. Venkateswaran, “Online Payment System using Steganography and Visual Cryptography”, Proceedings of the IEEE Conference on Electrical, Electronics and Computer Science, pp. 88-93, 2014.
[2] M. Naor and A. Shamir, “Visual Cryptography”, Advances in Cryptography -EUROCRYPT’94, Lecture Notes in Computer Science 950, pp. 1-12, 1995.
[3] Shamir,“How to Share a Secret”, Communication ACM, vol. 22, pp. 612- 613, 1979.
[4] G. R. Blakley, “Safeguarding Cryptographic Keys”, Proceedings of AFIPS Conference, vol. 48, pp. 313-317, 1970.
[5] Menezes, P. Van Oorschot and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, Boca Raton, FL, 1997.
[6] Borchert, “Segment Based Visual Cryptography”,WSI Press, Germany, 2007.
[7] W-Q Yan, D. Jin and M. S. Kanakanahalli, “Visual Cryptography for Print and Scan Applications”, IEEE Transactions, pp. 572-575, ISCAS-2004.
[8] T. Monoth and A. P. Babu, “Recursive Visual Cryptography Using Random Basis Column Pixel Expansion”, Proceedings of IEEE International Conference on Information Technology, pp. 41-43, 2007.
[9] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, “An Innocuous Visual Cryptography Scheme”, Proceedings of IEEE 8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.
[10] Blundo and A. De Santis, “On the contrast in Visual Cryptography Schemes”, Journal on Cryptography, vol. 12, pp. 261-289, 1999.
[11] P. A. Eisen and D. R. Stinson, “Threshold Visual Cryptography with specified Whiteness Levels of Reconstructed Pixels”, Designs, Codes, Cryptography, vol. 25, no. 1, pp. 15-61, 2002.
[12] E. R. Verheul and H. C. A. Van Tilborg, “Constructions and Properties of k out of n Visual Secret Sharing Schemes”, Designs, Codes, Cryptography, vol. 11, no. 2, pp. 179-196, 1997.
[13] H. Yan, Z. Gan and K. Chen, “A Cheater Detectable Visual Cryptography Scheme”, Journal of Shanghai Jiaotong University, vol. 38, no. 1, 2004.
[14] G. B. Horng, T. G. Chen and D. S. Tsai,“Cheating in Visual Cryptography”, Designs, Codes, Cryptography, vol. 38, no. 2, pp. 219-236, 2006.
[15] M. Hu and W. G. Tzeng, “Cheating Prevention in Visual Cryptography”, IEEE Transaction on Image Processing, vol. 16, no. 1, pp. 36-45, Jan-2007.
[16] "Common Cyber Attacks: Reducing The Impact" A Survey Report by CERT-UK https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf
[17] https://sentinelone.com/blogs/the-most-devastating-cyber-attacks-on-banks/
[18] https://en.wikipedia.org/wiki/Cyber-attack



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY