ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Detection and Prevention of Data Hacking in Net Banking Using Visual Cryptography Technique

Madhurani B Shiddibhavi[1], Pundalik Ranjolekar[2]

M.Tech Student, Dept. of Computer Science, KLE Dr. MSSCET, Belagavi, India[1]

Associate Professor, Dept. of Computer Science, KLE Dr. MSSCET, Belagavi, India[2]

ABSTRACT: In net banking system it is not guaranteed that every transaction will be carried out very much securely because of increasing the problem of hacking the data of authorized users. To provide security to such types of hacking activities in this project it aims to achieve the authenticity by visual cryptography technique namely 2 out of 2 scheme technique. It takes scanned signature image as an input. While creating new bank account, the bank will generate splits then bank will be given one split to user and another will be stored in bank database. The user needs to present the split during every transactions then the stacking of splits will be taking place. Decision of access granted or denied will be confirmed based on comparison of stacked and original image. If both are same then it will be confirmed that the user is authorized user otherwise unauthorized user.

KEYWORDS: Image processing; Visual cryptography; Authentication; Image stacking; Security; 2 out of 2 Scheme algorithm

I. INTRODUCTION

Banking system deals with number of transactions per day but it might have done using forging the original one unknowingly. Internet banking is not that secure in such case suspicious activities could be done by hackers. During the time of transaction username and passwords can be easily known to intruders. The main goal of this paper is to increase prevention of sensitive information within images. It should be protected by all types of hacking mal-wares on the web.

In this method the input is a signature image stored as a whole but the target will be to divide that image into number of splits which will have few characters inherited by the original image. The resultant image becomes subset of the main image. This splitting technique will accept the types of inputs such as any written text image, character image, and snap of a person. If a user may be in need of opening bank account, the user has to follow the instructions of filling all the details finally it asked for a user's signature for authentication purpose. The function of visual cryptography [1] starts from here. It will be made that image to divide to get user spilt as well as bank split. Internally the original image and bank split would be stored in bank database for the stacking purpose to obtain stacked image by overlapping with user split.

So this project is using this effective and efficient technique to get higher similarity and positive result. It helps to detect the frauds and the malicious activities running on the web. Finally it returns the optimistic outcome for better security.

II. RELATED WORK

The very first concept of secret sharing technique was introduced by Authors. The authors proposed this approach which could be applied on secret images [2] Contains sensitive information. This idea has implemented the method of dividing secret image in VCS [3]. In turn it returns number of shares but those created shares does not contain any information of original image data. It shows only about total size of the image. The authors could have collected the records for each input sample as soon as the stacking has been done. The authors have used logical operation OR to obtain the output. Authors were given 2 constraints where the output of desired system must satisfy these conditions.

- ❖ The divided image called share, it should be a legitimate subset of input image.

DOI: 10.15680/IJIRCCE.2016. 0406007

- ❖ That image should not give detail about sensitive information which was enclosed within it rather it has to disclose only about size of the image.

According to the author [4] has suggested cryptography which could be of type segment based. It would accept the inputs are of kind for ex, account no, balance available, and symbols. The authors named in [5] projected a policy of visual cryptography for printed text or image. The author had made the postulation that all customers will keep the shares confidentially do not disclosing to others truthfully. But this method did not check for the authenticity. So it returned inaccurate outcome. Author [6] implies the theory of Safeguard keys in cryptography. According to the author there were many data prevention schemes available. In cryptographic key usage enhanced the authentication of trusted user. The secret decoding can be processed some of the cryptography systems like RSA and DSA. Some keys would be stored in RSA and the administrator key and other few keys would be saved in DSA. This security mechanism was proposed by this author. Authors in [7] put up the concept of pixel expansion in recursive VC. In this technique the authors implemented column pixel extension on secret image thereafter it created number of shares and again the message could encode into n number of associated shares. Authors in [8] explained that, how to obtain the original data stored within images. Authors in [9] recommended the theory of digital watermarking. If the paper writing work is carried out in a group, each of them has to represent the respective work signified with watermarking technology. Authors in [10] introduced data matrix code it helps to detect the true possessor of data object. Authors in [11] tried to achieve great security by making use of CAPTCHA based on visual cryptography mechanism.

III. **PROPOSED ALGORITHM**

Step1: The proposed algorithm method is called as 2 out of 2 scheme technique which is based on visual cryptography. The secret image would be encrypted and generated n number of splits to avoid the complete data to be stored in single image. Rather it creates many splits for the purpose of managing data security in the form of splits.
Step2: The user is requested to register the name, address, account number, signature etc. Then the user has to submit these details to bank. The bank in turn stores this in database from database the bank obtained user's signature for creating splits and has been given to the user split to user. Another split was stored in the bank database. Now the overlapping will be taking place to form the stacked image. This will be compared with original signature stored in the database.

IV. **PROPOSED METHODOLOGY**

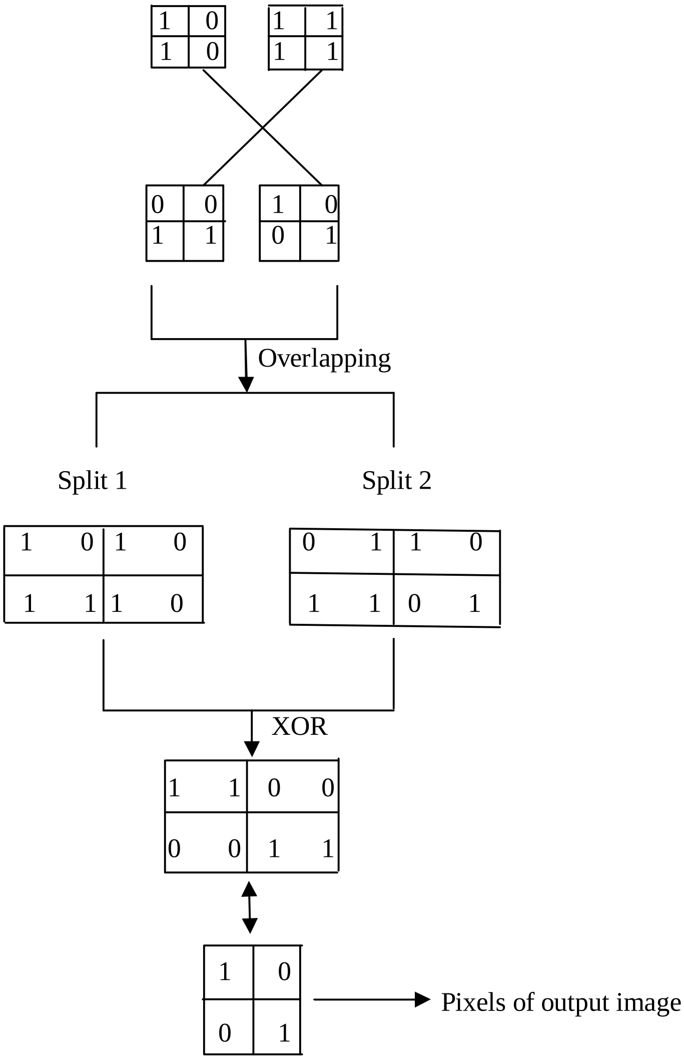
One of the encoding techniques is used to keep the information in secret within images then decoding the image using stacking. This technique represents the pixels in matrix form that is background pixel can be represented by 0 which is black in colour and data pixel can be represented by 1 which is white in colour. Upon overlapping if the resultant matrix contains subset of input matrix then it is said to be as true image. For example generally an image contains black and white pixels can be represented as

Pixels of input image $\longrightarrow \begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array}$

According to 2 out of 2 scheme visual cryptography technique, the below sub pixels are obtained.

Pixel separation	Splits	Sub pixels
0 – Black (Background pixel)	s1 s2	$\begin{array}{\|c\|c\|}\hline 0 & 1 \\ \hline 0 & 1 \\ \hline \end{array}$ $\begin{array}{\|c\|c\|}\hline 1 & 0 \\ \hline 1 & 0 \\ \hline \end{array}$ $\begin{array}{\|c\|c\|}\hline 1 & 1 \\ \hline 1 & 1 \\ \hline \end{array}$ Overlapping
1 – White (Data pixel)	s1 s2	$\begin{array}{\|c\|c\|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array}$ $\begin{array}{\|c\|c\|}\hline 0 & 0 \\ \hline 1 & 1 \\ \hline \end{array}$ $\begin{array}{\|c\|c\|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array}$

After overlapping the sub pixels, the bank will generate two splits as follows. Same pixels can give output as 0 and different pixels can give output as 1 according to XOR operation.



The output image becomes the subset of input image pixels hence the signature is authenticated and the user is authorized. Therefore user will be able to access the further transaction process.

V. PSEUDO CODE

*A. /*proposed 2 out of 2 scheme algorithm*/*

```
Step1: Read the scanned signature image as input of size 128X128 which should be in .bmp format.
Step2: Separate the data pixel and back ground pixel from the original image to obtain pre-processed image.
Step3: Obtain the matrix of pre-processed image and generate the splits.
Step4: Overlap the splits by stacking process.
Step5: Obtain stacked image called as post processed image.
Step6: Compare stacked image with input image in step1.
Step7: if (stacked_image = input image)
```

```
          then (" Allow access and authenticated successfully")
              else
Step8: if (stacked_image != input image)
          then(" Access denied and authentication failed")
Step9: End
```

B. Working and flow diagram of pseudo code

Banking systems allow user to interact with services only after sign in to the desired applications. If a user wants to open new account, the initial step to be taken by the user is to log in to the specific web site and open the application form which is already displayed by the bank as standard format to be filled by every user. Through this form the bank will take the signature for the purpose of authentication. It would be taken as a scanned image. This image itself is an input to the system. If the pre-processed image and stacked images are same after comparison then the user will be authorized and allows for access. Otherwise unauthorized and does not allow for access. This VC method provides complete accuracy while testing the system. In this method, the input scanned image will be divided into 2 splits. One split must keep with the bank and another split will be given to the user considered it as user's split. Since there are 2 splits, it is named as 2 out of 2 scheme technique. This is very efficient method to provide greater security for data within images. The pre-processed image and stacked image becomes similar hence result is proved and authentication is achieved. The flow of the VC technique has been shown below.

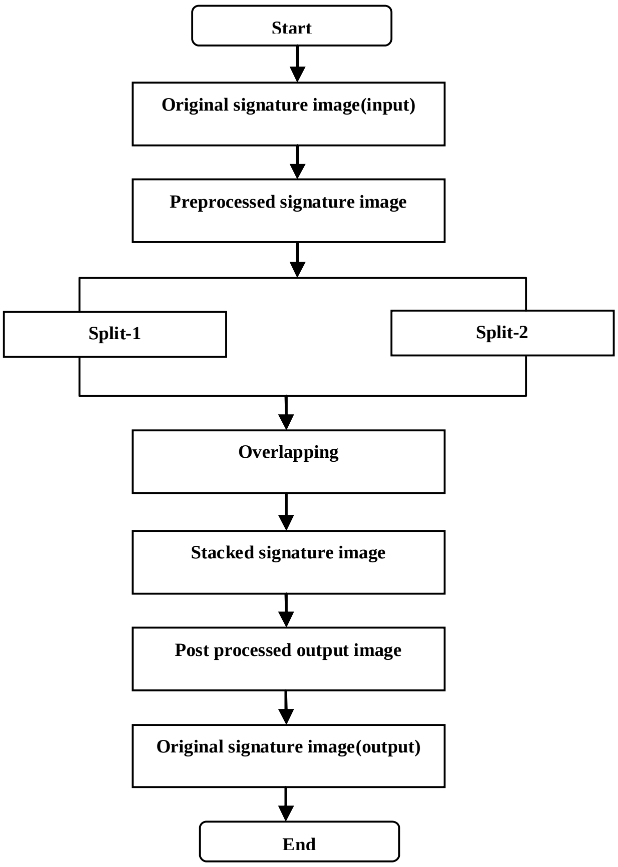

Start
Original signature image(input)
Preprocessed signature image
Split-1
Split-2
Overlapping
Stacked signature image
Post processed output image
Original signature image(output)
End

Fig1. Data flow diagram of visual cryptography

VI. EXPERIMENTAL RESULTS

Fig2. describes that initially the user has to provide authenticated data as an input to the bank admin. The user is providing scanned signature image for generating splits in the next step. This image contains noise in the input data that will be removed in the pre-processed step. The input image is given below.

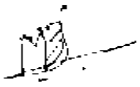
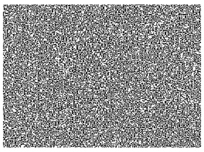


Fig2. Pre- processed signature image (Input)

In this step the Fig3 explains that the bank admin will create two splits and admin distributes those to user and bank itself. Fig4 explained that the bank's split will be stored in bank database itself. The user has to submit split which is belonging to respective user during every transaction process such as withdraw, deposit or any kind of money transfer tasks. The bank needs to check that whether the user is true and original or not.



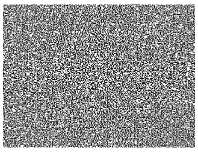


Fig3.Split-1(User split)   Fig4.Split-2 (Bank split)

Fig5 explains the final step of VC about post processed image which is nothing but stacked image. The admin will overlap the two splits for the verification of the true signature once after submitted to the bank. The stacked image gives subset or sub pixels of original image. If the obtained image will be independent of the subset then it could be declared that it is fake signature and user is not real user. If stacked image matches with input image then it could be said that the user is authorized one.

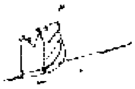


Fig5. Stacked signature image (Output)

The below table I explains the output results of some samples which are tested and obtained using the above algorithm. The users could access the data only when the correct split is submitted otherwise users will not allowed to access any services and those users might be considered as hackers or unauthorized users. This algorithm is implemented using java/ j2ee platform and produced very accurate output.

Table I. Results

Input samples	Tested Outcome
Signature sample 1	Authorized user allow access
Signature sample 2	Authorized user allow access
Signature sample 3	Un authorized user access denied
Signature sample 4	Authorized user allow access
Signature sample 5	Un authorized user access denied

VII. CONCLUSION AND FUTURE WORK

This paper is proposed the effective technique of visual cryptography in providing greater security for data stored within the images. Here the scanned signature image is an input to the application the bank will generate splits of input image using 2 out of 2 scheme VC technique. Then the bank distributes splits one to user and another is kept in bank database itself. Now the process of stacking is carried out to compare pre-processed signature with the post processed image of signature. The similarity level of signature decides the acceptation and rejection of user from transaction service. From this technique the secrete data authentication can be achieved and secure transactions can be done through the online service. This technique can also apply for photographs and colour images.

REFERENCES

1. C. 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.
2. M. Naor and A. Shamir, “Visual Cryptography”. Advances in Cryptography EUROCRYPT'94, Lecture Notes in Computer Science 950, pp. 1-12, 1995.
3. N. Anusha, and P. SubbaRao “Visual Cryptography Schemes for Secret Image”, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July – 2012.
4. B. Borchert,” Segment Based Visual Cryptography” WSI Press Germany, 2007.
5. W-Q Yan, D. Jin and M. S. Kanakanahalli, “Visual Cryptography for Print and Scan Applications” IEEE Transactions, pp.572-575, ISCAS-2004.
6. G. R. Blakley, “Safeguarding Cryptographic Keys”, Proceedings of AFIPS Conference, vol. 48, pp. 313-317, 1970.
7. T. Monoth and A.P Babu “Expansion of pixels” in Proceedings of IEEE International Conference on Information Technology, pp. 41-43, 2007.
8. 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.
9. 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, 1997.
10. Anushree Suklabaidya, and G. Sahoo,” Visual Cryptographic Applications”, IJCSE, Vol. 5 No, ISSN: 0975-3397, 06 Jun 2013.
11. P.S.Revenkar, Anisa Anjum, and W .Z.Gandhare, ”Secure Iris Authentication Using Visual Cryptography”, IJCSIS, Vol. 7, No.3, ISSN 1947-5500, 2010.

BIOGRAPHY

1. Ms. Madhurani Basavaraj Shiddibhavi is M-Tech student in Computer Science and Technology, KLE Dr. M.S.Sheshgiri College of Engineering and Technology of VTU University. She has received Bachelor of Engineering degree in 2012 from GEC Huvina Hadagali, India. Area of interests in Data mining and Image processing

2. Mr. Pundalik Ranjolekar is Associate Professor in Computer Science and Technology, College of KLE Dr. M.S.Sheshgiri College of Engineering and Technology of VTU University. He has completed the Bachelor of Engineering in UBDTCE Davanageri, India. Area of interests in Semantic webs, and Image processing.