VISUAL CRYPTOGRAPHY USING DES

Dr.E.Punarselvam[1], R.Gowsalya[2], T.Swetha[3], G.R.Priyadharshini[4], A.Sridharshini[5]

[1,2,3,4,5]*Department of Information Technology, Muthayammal Engineering College (Autonomous),Tamilnadu*

Abstract:-Visual cryptography is protecting text based secret. As network technology has been greatly advanced, much information is transmitted via the Internet conveniently and rapidly. At the same time, the security issue is a crucial problem in the transmission process. In this project we proposed a visual cryptographic system using DES. In this DES algorithm, Encryption and Decryption provides solution for both individuals and corporations. Using this algorithm, user can easily encrypt and decrypt text (messages), so you can send emails safely. The proposed method is a simple, practical and effective cryptographic system. The text information is encrypted and stored in the Color Palettes. Whenever the user has decrypted their encrypted information, they should enter the correct secret key. Users send any secure information, it was encrypted and its link is sent to the mail. If the recipient enters wrong key, get an error message "Wrong Secret key".

I. INTRODUCTION

This proposed system using DES algorithms, text information is encrypted by color palette images. Each user has created individual account, and then they access their required pages. The user's password is converting into ASCII format and stored into the database. So any hackers or admin also should not find out the particular user's password details. The user's information is protected into specific secret key entered by user. The secret key is converting into ASCII format and stored to database. Whenever the user has decrypted their encrypted information, they should enter the correct secret key. And users send any secure information, it was encrypted and its link only sent to the mail.

We propose a secure display technique based on visual cryptography. The proposed technique ensures the security of visual information. The display employs a decoding mask based on visual cryptography. Without the decoding mask, the displayed information cannot be viewed. The viewing zone is limited by the decoding mask so that only one person can view the information. We have developed a set of encryption codes to maintain the designed viewing zone and have demonstrated a display that provides a limited viewing zone.

The basic problem of visual cryptography by a visual variant of the *k* out of *n* secret sharing problem: how can an original picture are encoded by *n* transparencies so that less than *k* of them give no information about the original, but by stacking *k* of them the original can be seen? They described a solution to this problem by a structure called *k* out of *n* secret sharing scheme whose parameters directly correspond to quality and usability of the solution.

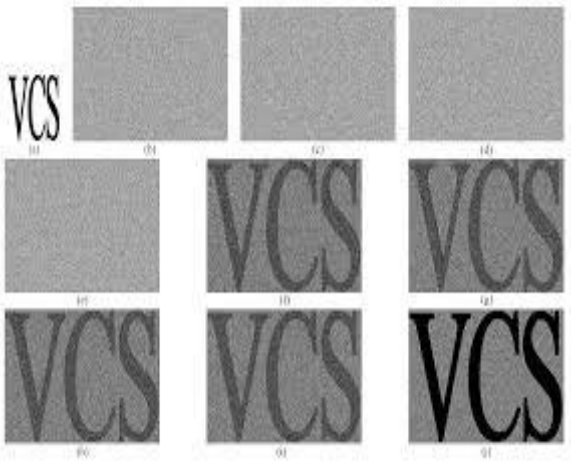

Figure 1.1

II. SYSTEM DESIGN

In the proposed system, DES algorithm used for both encryption and decryption process. Each user has an individual account in the website. User's password converted into ASCII format and saved into the database. Encrypted and Decrypted information are stored in Color palette. Whenever the user decrypted their encrypted information, they should enter the correct secret key. User send any secure information, it was encrypted and its link sent to the mail.This process worked on any online domain otherwise, we will try to install the SMTP protocol.

We have developed a set of encryption codes to maintain the designed viewing zone and have demonstrated a display that provides a limited viewing zone. We propose a secure display technique based on visual cryptography. The proposed technique ensures the security of visual information.

IMPLEMENTATION

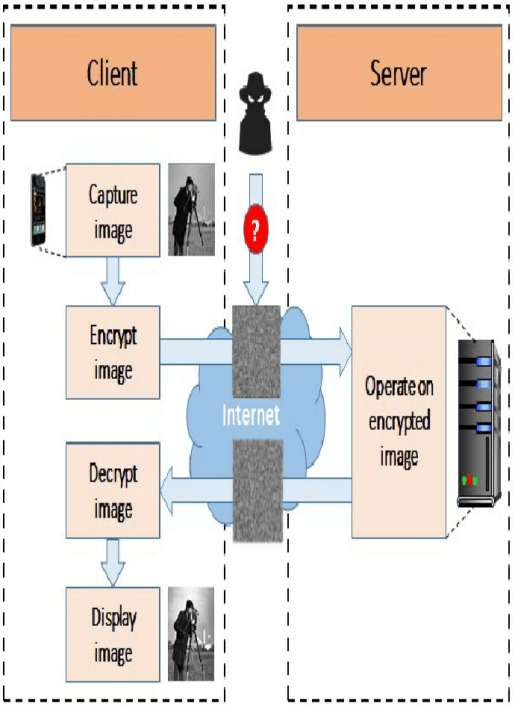

Figure 1.2

IMPLEMENTATION PROCEDURES

After proper testing and validation, the question arises whether the system can be implementation or not. Implementation includes all those activities that take place to convert from old system to new.

The new system may be totally new replacing an existing system. In other case, proper implementation is essential to provide a reliable system to meet organization requirements.

USER TRAINING

A well-designed system, if not operated and used properly could fail. Training the users is important, as if not done well enough could prevent the successful implementation of an information system. Through the system development life cycle the user has been involved. By this stage the analyst should possess an accurate idea of the users they need to be trained.

They must know what their roles will be, how they can use the system and what users need training. During their training, they need to be given a trouble-shooting list that identifies possible problems and identifications that may arise and how to solve them.

OPERATIONAL DOCUMENTATION

Once the implementation plan is decided, it is essential that the user of the system is made familiar and comfortable with the environment. Education involves right atmosphere & motivating the user. A documentation providing the whole operation of the system is being developed. The system is developed in such a way that the user can work with it in a well consistent way.

The system is developed user can work the system from the tips given in the application itself. Useful tips and guidance is given inside the application itself to help the user. Users have to be made aware that what can be achieved with the new system should be given a general idea of the system before he uses the system.

CREATE COLOR PALETTE IMAGE

The module, small color images are created by PHP GD functions. Each text has assigned to particular images. The color palette images and its relevant information are stored into the database.

ENCRYPT THE TEXT

In this module the user has to register their name and their details. The registered information will be stored in the database. User or administrator tries to check this site and entered correct login username and password. After that, this application checks to redirects the required pages for administrator as well as user. The user has entered their important information, each text has convert to particular images. The images are randomly allocated to each text. Then image names only stored to database.

SEND THE ENCRYPTED TEXT TO MAIL WITH WEB LINKS

In this module the user enter the information, and then send to particular mail address. User's information is stored into the database for encrypted format. So web link with information's ID only sent to the mail. The mail has sent by SMTP protocol. This process only worked on any online domain. Otherwise we will try to install the SMTP protocol.

RETRIEVE THE WEB LINKS FROM MAIL

In this module receiver is click this link, then open into this website. The receivers enter the secret key, if it is check with database, after they will retrieve the decrypted information.

DECRYPT THE TEXT

In this module the base, these information displayed only color palette format. After the user is enter the secret key, if there are compare with database, and the information is decrypted. Then the user is view their information.

FEEDBACK

In this module, the user has to give their comments and feedback about this site. This information will be watched by admin.

FEASIBILITY STUDY

Feasibility study is made to see if the project on completion will save the purpose of the organization for the amount of work, effort and the time that on it. Feasibility study lets the developer for see of the project and the usefulness feasibility study of the system proposal is according to its workability, which is the impact on the organization, ability to meet their user needs and effective use of resource. Thus when a new application is proposed it normally goes through a feasibility study before it is approved for development.

Three key consideration involved in the feasibility analysis are

1. Economic feasibility
2. Technical feasibility

1. Economic Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the organization can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well as within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

2. Technical Feasibility

This study is carried out to check the technical feasibility that is the technical requirements of the system. Any system developed must not have high demand on the available technical resources. This will lead to high demand on the available technical resource. This will lead to high demands being placed on the organization.

The developed system must have a modest requirement, as only minimal or null changes are required for implementing the system.

SYSTEM MAINTENANCE

A system should be created whose design is comprehensive and farsighted enough to serve current and projected user for several years to come. Part of the analyst's expertise should be in projecting what those needs be in building flexibility and adaptability into the system.

The better the system design, the easier it will be to maintain and the maintenance costs is a major concern, since software maintenance can prove to be very expensive. It is important to detect software design errors early on; as it is less costly than if errors remain unnoticed until maintenance is necessary. Maintenance is performed most often to improve the existing software rather than to respond to a crisis or system failure. As user requirements change, software and documentation should be changed as part of the maintenance work.

Maintenance is also done to update software in response to the change made in an organization. This work is not as substantial as enhancing the software, but it must be done. The system could fail if the system is not maintained properly.

III. RESULT AND DISCUSSION

User has to register their name and details. The registered information will be stored in the database. User checks their account by entering the correct login username and password. The administrator authenticates, whether it is correct or not.

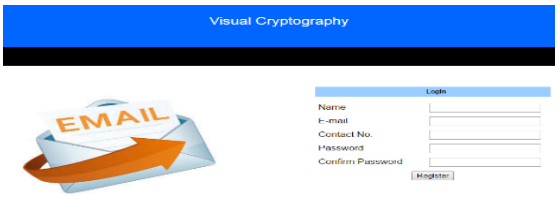

Figure 1.3

Figure 1.4

User enters the information, and then send to particular mail address. User's information stored into the database in encrypted format.

Figure 1.5

User's secret information are stored into the database, these information displayed only in color palette format. The receiver enters the secret key, it compares with the database, whether, it is correct then information is decrypted otherwise, not decrypted.

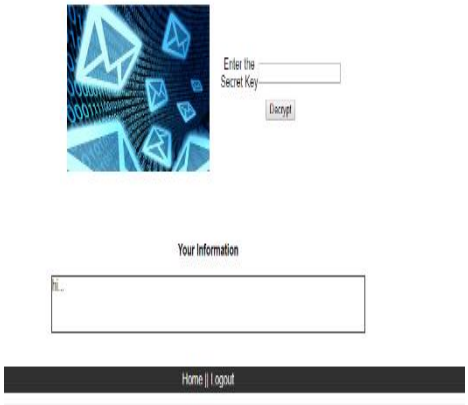

Figure 1.6

IV. CONCLUSION

We can conclude that the text information is safely sent from sender to the receiver. Visual Cryptography method is used for protecting text based secrets. This method is simple, practical and efficient cryptography method. This project helps to secure user's information, safely encrypt and decrypt the text. Here, DES algorithm provides high security for text. Your device and your personal data are safe. It provides more accuracy of sharing text.

V. REFERENCES

[1] Pandya, R., Patel, J. Patel, B. Patel "Image Password Based Security System" International Conference on Current Research Trends in Engineering and Technology, 2018

[2] E.Punarselvam,"Different loading condition and angle measurement of human lumbar spine MRI image using ANSYS", Springer Journal of Ambient Intelligence and Humanized Computing, ISSN 1868-5137, https://doi. org/10.1007/s12652-020-01939-7

[3] Taiwan National Central University, Jung Li, 320, ROC Received 6 June 2002, accepted 26 August 2002.

[4] Dr.J. Preetha and Dr.S.Lavanya" Security Based Service Infrastructure for Wireless Adhoc Networks using Fuzzy Logic" PAIDEUMA JOURNAL OF RESEARCH, ISSN No: 0090-5674 at Volume-XIII Issue-II, FEBRUARY 2020Pg:103-108

[5] Yang CN, Tung TC, Wu FH, Zhou Z, "Color transfer visual cryptography with perfect security" Measurement. 2017 Jan1;95:480-93.

[6] E.Punarselvam, "Edge Detection of CT scan spine disc image using canny edge detection algorithm based on magnitude and edge length", 3rd International Conference on Trendz in Information Sciences & Computing (TISC2011), 15 March 2012, PP(136-140) DOI: 10.1109/TISC.2011.6169100

[7] E.Punarselvam, "Big Data using Hadoop Database using python Language to implement Real Time Applications", International Journal of Engineering Research and development,Vol.8 Issue No.12 Oct 2013 PP(19-22) e-ISSN:2278-067X,p-ISSN:2278-800X.

[8] .E.Punarselvam,"Effective and Efficient Traffic Scrutiny in Sweet Server with Data Privacy", International Journal on Applications in Information and Communication Engineering Volume 5 : Issue 2: November 2019, PP 1 – 5

[9] HaoLuo, Hua Chen, Yongheng Shang, Zhenfei Zhao, Yanhua Zhang "Color Transfer in Visual Cryptography" Measurement 51(2014), 81-90, 27 January,2014

[10]E.Punarselvam,'Non-Linear Filtering Technique used for Testing the Human Lumbar Spine FEA Model', in Journal of Medical Systems (Springer), vol. 43, no. 2, pp. 1-13.ISSN 0148-5598 DOI:10.1007/s10916-018-1148-6 .Impact Factor 2.098.

[11]Young Chang Hou, Zen Yu Quan and Hsin-Yin Liao "New design for friendly visual cryptography" International Journal of Information and Electronics Engineering, Vol. 5, No. 1, Jan2015.

[12]E.Punarselvam,"Segmentation of Lumbar spine image using Watershed Algorithm", International Journal of Engineering Research and Applications",Vol.3 Issue No.6 Dec 2013 PP(1386-1389) ISSN:2278-ISSN:2248-9622.

[13]Li Shundong, LI Jiliang,WANGDaoshun "Region Incrementing Visual Cryptography with same contrast" Chinese Journal of Electronics ,Vol 25, No. 4,July2016

[14]E.Punarselvam,"Investigation on human lumbar spine MRI image using finite element method and soft computing techniques", Springer Journal of Network, Software Tools and Applications, ISSN(Online) : 1386-7857 Cluster Computing DOI 10.1007/10586-018-2019-0

[15]S.Srividhya, R.Satishkumar, Gnanou Florence Sudha "Implementation ofTiOISSSwith meaningful shadows and with an additional authentication image" J.Vis.Commun.Image R., accepted 8 March2016.

[16]MoniNaor and Adi Shamir "A Visual Cryptography" in proceedings of Advances in cryptology, EUROCRYPT 94, Lecture notes in computer science,1994.