International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072

A Stroke concealed point method with integrated approach of Asymmetric Cryptography and Steganography

T.M.Venkatesh[1], N V Vishnuvardhan[1], S.Srinivasan[1], G Muneeswari[2]

[1]*Student, Dept. of Information Technology, SSN college of Engineering*

[2]*Associate Professor, Dept. of Information Technology, SSN college of Engineering*

Abstract- ***For information and computer security passwords are used. Commonly used passwords are alphanumeric passwords, which are combination of alphabets, numbers and some special characters. These types of passwords are vulnerable to various attacks. To have more secured passwords graphical passwords are introduced. Even though graphical passwords are more secure, it also has usability problems. Since it can be overcome by practice and also easy to remember its usage is increasing. But, Shoulder Surfing is one of the threats to graphical passwords, where the attacker will capture the password by direct observation. To overcome this problem some known defense technique is used, along with Steganography. Steganography is a technique in which the information is hidden in digital media like images, video, audio, etc. Image Steganography is the most commonly used technique in which the information is hidden in an image. LSB method is efficient algorithm to hide information in the cover image. In this paper, Draw A Secret (DAS) is used as a graphical password. To avoid shoulder surfing disappearing strokes technique is used in DAS. The data is steganographed with DAS image and sent to server. In server side, it is de-steganographed and data is verified with database.***

Key Words- Graphical password, Shoulder surfing, Draw A secret (DAS), Steganography, LSB.

1. INTRODUCTION

In modern days, login sessions are insecure. The traditional alphanumeric password is facing a severe vulnerability due to increasing attacks on these type of passwords. In addition to this, some strong alphanumeric passwords are difficult to remember.However , the graphical passwords are easy to remember and relatively less prone to the attacks. So graphical passwords are better alternatives for alphanumeric passwords. Graphical passwords are recognition based, recall based and cued-recall based. In this paper we will discuss about the Draw A secret (DAS) password which is a recall based graphical password. Even Draw A secret(DAS) password suffers from three security problems like Multiple Accessed Passwords, Graphical dictionary attacks and Shoulder surfing attacks.

1. In Multiple Accessed Passwords, more than one password is accepted because of less number of cells in the grid.

2. In Graphical dictionary attack, the password is being guessed by the attacker by 'point of interest'.

3. In Shoulder surfing attack (SS), the attacker can crack the victim's password by directly observing the password.

During authentication sessions hackers attempt to crack passwords. While payment processing period, the hackers attempt to have access to sensitive information. To further increase the security of the password, Steganography and Cryptography are used.

The concept of cryptography is about the plain text which is encrypted with a shared secret key and converted to cipher text and this cipher text is decrypted on server side with the same key.

But even these systems are vulnerable to hacking since the existence of a message is known to hackers. There are many techniques to crack the cipher text. So we go for a concept where message existence should not be known. This can be implemented by Steganography.

Steganography is a concept of concealing a message passed to server. This is done by hiding information in an image with help of stego key. In this method, if the existence of message is known then it can easily be desteganographed and information is retrieved since information is raw

message and not encrypted. So it is not secure even though it is concealed.

In this paper, a concept of hybrid technology is introduced where the concepts of Steganography and cryptography are combined. So it increases the difficulty to hack the message.

2. RELATED WORKS

The review of shoulder surfing defense concept incorporates vast number of advancements and developments, among which few are discussed in this section. Nowadays, traditional alphanumeric passwords for authentication are in practice. [1] elucidates clearly about the graphical password system(GPS) known as the passpoints as an alternative for the text based passwords which can be hacked easily if it is a short password whereas it is difficult to remember a long password. GPS can be implemented by Draw a Secret Scheme which is shown in [2].In this scheme the password is drawn according to a stroke sequence which is sequence of cell crossings bounded by both ends by pen-up events on a rectangular grid based keypad. Though GPS poses several advantages, it is susceptible to certain graphical password attacks such as SS which is depicted in [3]. It analyzes the SS risk of perceived and real configurations of graphical password, Passfaces[4] which revolves around the concept of using a computer generated random images of human faces for authentication.

Therefore defense technique was implemented for SS as in [5] which explains about method in which the strokes drawn on the grid can be made to disappear quickly after completing the drawing of each stroke sequence. According to experiment conducted on discerning out better method for SS defense among decoy strokes, disappearing strokes and line snaking and also based on weak, medium and strong password strength, the following results were drawn. The best solution for SS defense was disappearing strokes with strong password strength.

The data transmitted by the sender suffers security problems as it gets hacked by the hackers. Hence [6] elucidates the method for hiding the data with help of encryption and is converted to cipher data which is known as cryptography. There are two different types of cryptography such as symmetric and asymmetric cryptography. In [7] symmetric method, the sender and receiver shares the same key to encrypt and decrypt respectively whereas in [8] asymmetric both are provided with disparate keys which can be either public-private key or private-public key to enhance security levels of the transmitted data but it is slower compared to symmetric encryption.

The single encryption method can also be extrapolated to multiple encryption in [9] by using hybrid of three methods of encryption standard methods such as Advanced encryption standard(AES),Rivest-Shamir-Adleman(RSA) and Chaotic pseudo random sequence(CPRS). But this method again suffers from security problems since the existence of message transmitted is known to the hackers. So the existence of message is made unknown by hiding the data inside an image applied with a key. This method is known as Steganography as depicted in [10] where it is applied with stego key. Steganography can be implemented through various methods and one such method is Least significant bit(LSB) which is discussed in [11]. Here the LSBs of each pixels of cover image are replaced by LSBs of each pixels of secret message thereby obtaining stego image which is applied with stego key and then transmitted to receiver. In [12],other methods are Most significant bit method ,Jsteg,Outguess which is used for implementation of Steganography.

3. DRAW A SECRET SCHEME –AN ALTERNATIVE METHOD FOR ALPHANUMERIC PASSWORDS

Draw a secret scheme is a scheme which uses graphical passwords for login sessions replacing the traditional alphanumeric password. This method allows users to use a set of gestures drawn on the grid for authentication. The user's diagram is mapped on to N*N grid denoted by discrete rectangular coordinates (x,y) which are recorded in ordered sequence of cell while user is constructing the secret. At the end of one stroke new coordinates are inserted to the recorded sequence and another stroke begins on the grid.

Graphical passwords are favorable compared to traditional alphanumeric passwords according to picture superiority effect which describes performance of human mind in recalling images & ob0jects compared to strings of text. So stronger and secure sequences can be recorded through graphical password schemes compared to alphanumeric passwords. This scheme offers users a sufficient tolerance level during authentication such that cell sequence follows the same encoding even though the diagram does not match exactly the originally recorded sequence of cells while constructing a secret. A drawing secret will be disallowed if it crosses through a cell corner or traces the

grid lines. This is called as illegal crossings or fuzzy boundaries.

A stroke consists of sequential cell crossings which is bounded at both ends by pen up events. Example: Consider a rectangular 5*5 grid with stroke count 2 and first stroke sequence (1,5); (1,4); (1,3);(2,3);(3,3);(3,4);(4,4);(4,5);(5,5) of stoke length 9 and another sequence (2,1); (3,1); (3,2); (3,3); (4,3);(4,2) of stroke length 6 as shown in the figure-1.

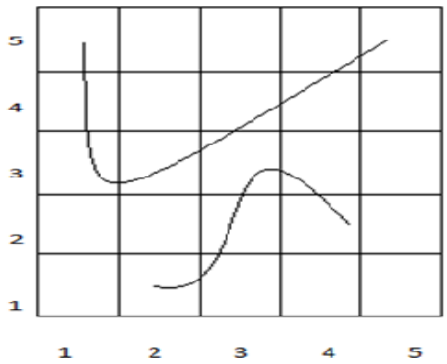

Fig-1: 5*5 grid for drawing DAS

The length of the stroke is the number of coordinate pairs it contains. The length of a password is sum of length of its component strokes(in Fig-1 password length is 15).The number of strokes and password length are important security metrics in measuring strength of a password(weak, medium or strong).A high number of strokes and high password length is the most secure password. A secured password is based on two factors: usability & defensive. The DAS passwords faces a problem, as the free form picture of N*N grid can be easily memorized by person nearby. So it suffers from shoulder surfing. The other problem is usability where users have to draw the diagram exactly as originally encoded graphical password and avoiding illegal crossing.

3.1. DEFENSE TECHNIQUE - A STROKE CONCEALED POINT METHOD

A defensive technique to avoid shoulder surfing in Graphical passwords(DAS) is coined in this paper. This technique is called a stroke concealed point algorithm. In this algorithm the user first draws the strokes on the screen for DAS. The method employed here is that when the user draws the strokes the user sees only the points in the screen. The points are intersection of strokes with the grid in the DAS screen along with starting and ending points in the stroke. The points are generated as the user draws the password. However this algorithm is not applied while the user setting his password. This algorithm is applied during the login session where the user enters this password for authentication. The view of password while setting it and while using it for authentication are depicted in Fig -2(a) and Fig -2 (b) respectively. This method is secure as the other persons behind the user gets befuddled with graphical password in the form of points instead of strokes and they also find it difficult to store in their memory.

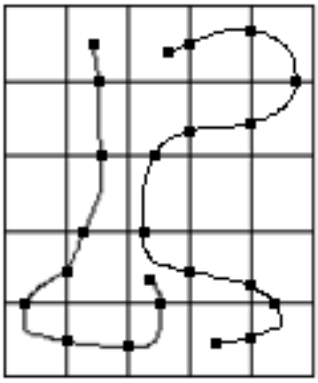

Fig-2(a): Strokes drawn by the user on the rectangular grids.

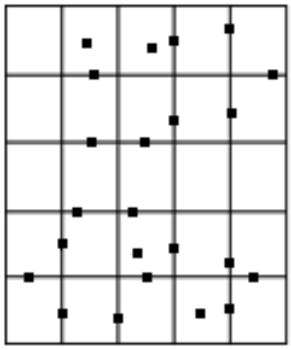

Fig-2(b): Strokes visible only in the form of points according to others behind the user.

4. ASYMMETRIC CRYPTOGRAPHY BY USING PRIVATE-KEYS

Cryptography is a technique in which the conversion of plaintext into cipher text is done by some encryption algorithm and at the receiver end, the cipher text is received and decrypted into plaintext. This helps in sending information securely. The sender or receiver uses

keys to encrypt or decrypt the plain text .There are two types of keys ,symmetric and asymmetric. If the sender and receiver shares the same key to encrypt and decrypt respectively ,then the key used is known as symmetric key. In asymmetric key method the sender and receiver uses a key-pair in which both the keys are different. Either key-pair can be public key-private key or private key-public key. This method is said to be asymmetric encryption. In this paper we are using asymmetric encryption with the help of a private key. The asymmetric key technique are explained in Fig-3 respectively

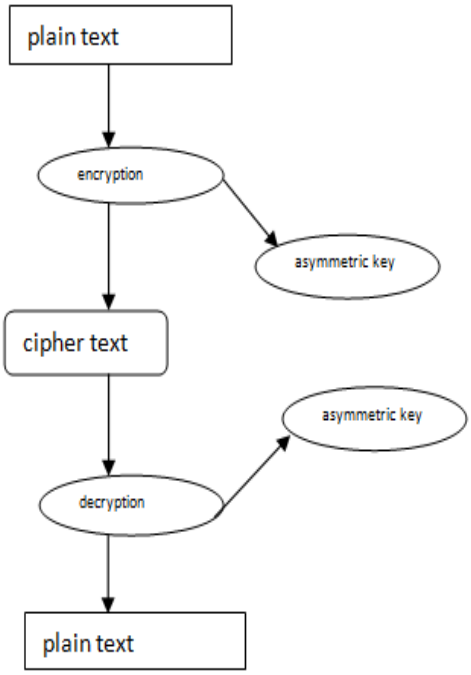

Fig-3: *CRYPTOGRAPHY* using *asymmetric key*

5. STEGANOGRAPHY BY LSB METHOD

Steganography is a technique in which the information is concealed in media. The media can be audio, video, image, text etc. In this paper we are discussing about image Steganography in which information is concealed inside a cover image using stego key which turns into stego image. The cover image used in Steganography is the graphical password, i.e., DAS drawn during the login session is converted into a bitmap image and used for concealing the information which is username itself.

LSB technique is one of the most frequently used techniques to hide the information in an image. In this technique, the secret message is converted into binary. The LSB of the cover image is replaced by each bit of secret message to form stego image. At the receiver the message can be retrieved from the stego image.

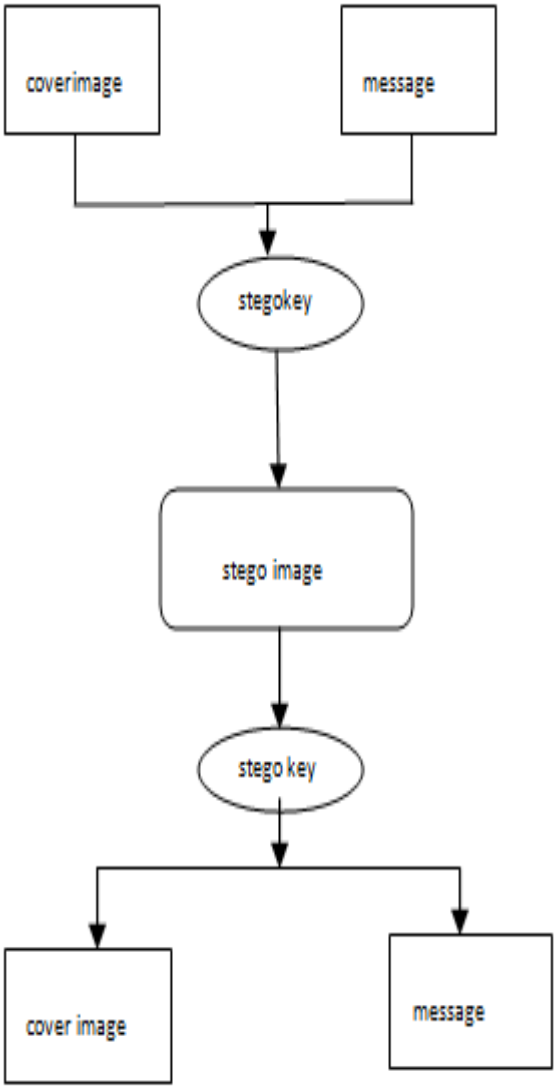

Fig-4: Steganography and De-steganography technique

Above Fig-4 explains the steganography technique and how the message is retrieved from a stego-image. The stego-key has the information of algorithm used to embed the message to the cover image. The same stego key should

be used in the receiver end to retrieve the message from the stego image.

6. METHODOLOGY FOR SECURE LOGIN AND USER-SERVER INTERACTION SESSIONS

During login sessions the user is authenticated using graphical password which is DAS. But as DAS suffers from shoulder surfing we present a new technique called stroke concealed point algorithm as depicted in this paper. The strokes are drawn in a 5*5 grid. The username entered by the user during login or any user-server interaction messages which contains sensitive information, for example, transaction of amount during payment processing after login acts as the secret message which is encrypted to cipher text by asymmetric encryption.

The cipher text used as the message has to be hidden in the cover image. The message is hidden using the LSB technique of image steganography using stego key. Here the graphical password drawn acts as the cover image in steganography process. This steganographed image is then sent to the server for validation.

The steganographed image is received at the server undergoes a process of de-steganography, where the stego image is desteganographed using the stego key. This process gives the DAS image and the cipher text which contains the username or the user-server interacted message. The cipher text is decrypted using the asymmetric key to retrieve message or username. The username and the graphical password are checked for validity. If it is valid, i.e., the username and graphical password matches then it results in successful login. Else it fails. There is no check for validation in case of user-server interacted messages. The process taking place in user level and server level is explained in Fig-5(a) and Fig-5(b) and the process taking place after login is explained in Fig-5(c).

AT USER LEVEL

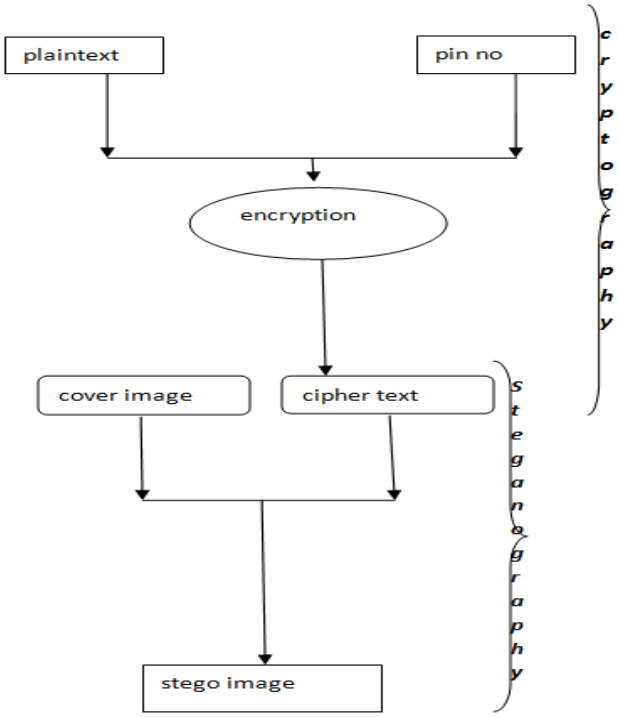

Fig-5(a): Authentication Process At User Level

AT SERVER LEVEL

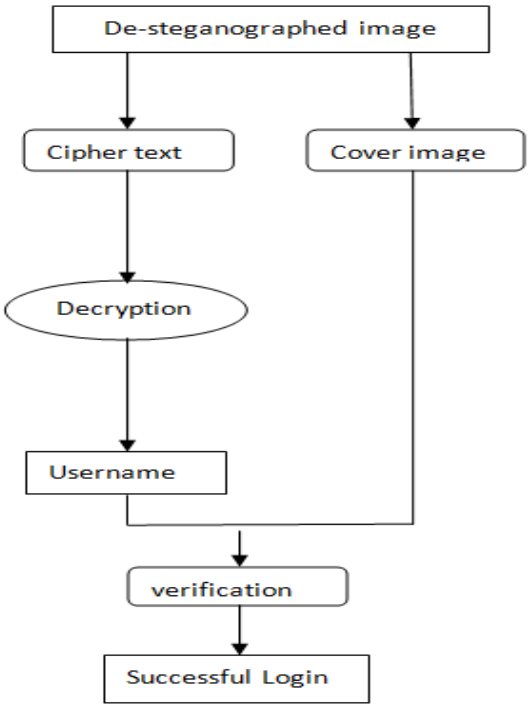

Fig-5(b): Verification Process At Server Level

AFTER LOGIN (for transferring sensitive information)

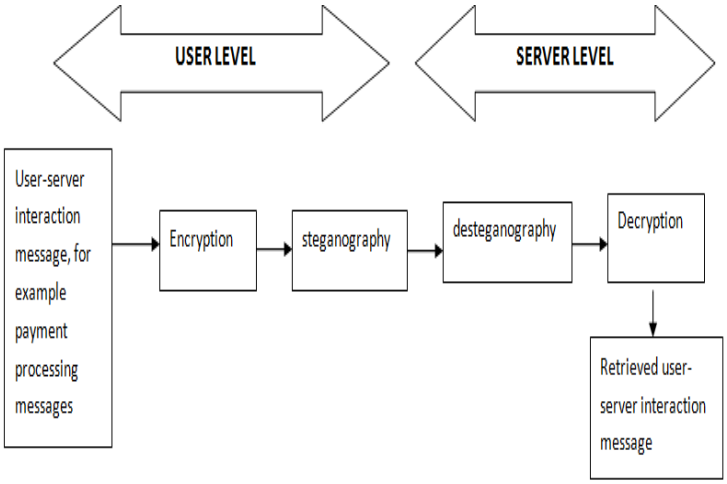

Fig-5(c): Process for user-server interaction messages after login.

7.CONCLUSION AND FUTURE ENHANCEMENTS

The data that is being authenticated during login session is being attacked easily by hackers as the security levels of traditional method of using alphanumeric passwords are slightly low. So the alternate graphical password(DAS) with defense technique for shoulder surfing using a hybrid technique is coined in this paper. The hybrid technique uses steganography along with cryptography to have an incremental effect on security levels in login sessions as well as user-server interaction sessions.

The proposed idea as presented in this paper can be further enhanced by the research made on multi level encryption instead of standard encryption method by using chaotic mapping and DNA coding where more security is established during transmission and reception of data. The LSB technique used for steganography is not robust, i.e., it is very sensitive to filtering. And the attacker can destroy the message in the stego image by changing the LSB of the stego image. Thus improvement can be done to LSB technique or an alternative steganography technique can be used to overcome this problem. The defense technique used to prevent shoulder surfing suffers usability problem on which further work can be done.

9. REFERENCES

[1]Authentication Using Graphical Passwords: Basic Results- Susan Wiedenbeck Jim Waters ,College of IST ,Drexel University; Jean-Camille Birget, Computer Science Department, Rutgers University; Alex Brodskiy Nasir Memon ,Computer Science Department Polytechnic University Brooklyn, NY,USA.

[2] Shoulder Surfing attack in graphical password Authentication:Arash habibi lakshari, Computer Science and Data Communication (MCS),University Malaya (UM)Kuala Lumpur, Malaysia ; Samaneh farmand,Computer Science and Information Technology (IT),University Malaya (UM) Kuala Lumpur, Malaysia.

[3]Impact of Background Images on the DAS (Draw- A- Secret) Graphical Password Authentication Scheme-Y.D.S.Arya and Gaurav Agarwal Invertis University, India

[4] F. Tari, A. A. Ozok,and S. H. Holden. 2006. A Comparison of Perceived and Real Shoulder-surfing Resistant Risks between Alphanumeric and Graphical Passwords. In

Proceedings of the Second Symposium on Usable Privacy and Security (Pittsburgh, PA, USA, July 12-14, 2006), ACM Press, New York.

[5] P.Dunphy and J.Yan. 2007. Do Background Images Improve "Draw a Secret" Graphical Passwords? In Proc. of the 14th ACM Conference on Computer and Communications Security(Alexandria, Virginia, USA, October, 28-31, 2007). ACM Press, New York, 36-47.

[6] Wenbo Mao. Modern cryptography: Theory and practice. Prentice Hall, 1st edition, 2003.

[7]A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data-Sarker, M.Z.H. ; Dept.of CSE, East West Univ., Dhaka ; Parvez, M.S.

[8] Fanfara, P. , Dankova, E. , Dufala, M,Dept. of Comput. & Inf., Tech. Univ. of Kosice, Kosice,Slovakia :Usage of asymmetric encryption algorithms to enhance the security of sensitive data in secure communication.

[9] A Secure Communication System with Multiple Encryption Algorithms-Jian, Wang ; Dept. of Electron. Sci. & Eng., Nanjing Univ., Nanjing,China ; Liu Xu ; Xiaoyong,ji

[10] N. Johnson, Digital Watermarking and Steganography: Fundamentals and Techniques , The Computer Journal. (2009)

[11] P. Watters and F. Martin and H. Steffen Stripf. Visual Detection of LSB-Encoded Natural Image Steganography. In ACM Transactions on Applied Perception, Vol. 5, No. 1, Article 5, 2008.

[12] Combining Steganography and Cryptography: New Directions- Khalil Challita and Hikmat Farhat, Computer Science Department, Notre Dame University - Louaize, Lebanon.

[13] V. Roth, K. Richter, and R. Freidinger. 2004. A PIN-Entry Method Resilient Against Shoulder Surfing. In Proceedings of the Computer and Communication Security (Washington DC, USA, October 25-29, 2004), ACM Press, New York 236-245.

66.

[14] A. Forget, S. Chiasson, and R. Biddle. 2010. Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords. In Proceedings of the 28th International Conference on Human Factors in Computing Systems (Atlanta,GA, USA, April 10-15, 2010). ACM Press, New York, 1107-1110).

[15] Nur Haryani Zakari Griffiths, School of Computing Science, Newcastle University, UK Dept. of Information Engineering, SachaBrostoff, Chinese University of Hong Kong, Jeff Yan,
Dept. of Computer Science, University College London, UK-Shoulder Surfing Defence for Recall-based Graphical Passwords

[16] B. Chen and G.W.Wornell. Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding. In IEEE Trans. Information Theory, volume 47, no. 4, pages 1423–1443, 2001.

[17] N. Hopper and L. Von Ahn and J. Langford. Provably Secure Steganography. IEEE Transactions on Computers, volume 58, number 5, 2009

[18] B. Dunbar. A detailed look at steganographic techniques and their use in an opensystems environment. Sans InfoSec Reading Room, 2002.

[19] T. Jahnke, J. Seitz, (2008). An introduction in digital watermarking applications, principles and problems, in: H. Nemati (Ed), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 554-569.

[20] International Journal of Advanced Research in Computer Science and Software EngineeringA New Approach to Hide Text in Images Using Steganography Vipul Sharma,School of Computer Science & Engineering Bahra University, Shimla Hills, India.Sunny Kumar,School of Computer Science & Engineering Bahra University, Shimla Hills, India.

[21] Katzenbeisser and Petitcolas. Information hiding: Techniques for steganography and watermarking. Artech House, 2000.

[22] Z. Li, Q. Sun, Y. Lian, and D. D. Guisto. 2005. An Association-Ba Graphical Password Design Resistant to- Shoulder Surfing Atta In Proceedings of the IEEE International Conference on Multime and Expo (Amsterdam, The Netherlands, July 6-8, 2005) IE Computer Society, 245- 248

[23] Bruce Schneier. Applied Cryptography:Protocols, Algorithms, a Source Code in C. In Wiley, 2nd Edition, 1994.

[24] Katiyar.S. , Meka, K.R. ; Barbhuiya, F.A. ; Nandi, S. Dept. of Comput. Sci. & Eng., Indian Inst. of Technol. Guwahati,

Guwahati, India , Online Voting System Powered by Biometric Security Using Steganography.

[25] A Multilevel Image Encryption Algorithm Based on Chaos and DNA Coding Qian Wang, Qiang Zhang*, Changjun Zhou Key Laboratory of Advanced Design and Intelligent Computing, Dalian University.

10.BIOGRAPHIES

The Author is currently studying 3rd year B.Tech.(Information Technology) in SSN College of Engineering, Kalavakkam, Chennai, Tamilnadu. Fields of interest are Security and Networks.

The Author is currently studying 3rd year B.Tech.(Information Technology) in SSN College of Engineering, Kalavakkam, Chennai, Tamilnadu. Fields of interest are Security and Networks.

The Author is currently studying 3rd year B.Tech.(Information Technology) in SSN College of Engineering, Kalavakkam, Chennai, Tamilnadu. Fields of interest are Security and Networks.

The Author is currently working as Associate Professor in Information Technology Dept., SSN College of Engineering, Kalavakkam, Chennai, Tamilnadu.

