

# Implementation Of Video Object Steganographic Mechanism For Remote Authentication Using Biometric

Ms.M.N.Narote<sup>1</sup>,Prof.S.K.Korde<sup>2</sup>.

<sup>1</sup> PG Student, Computer Department,PREC,Maharashtra,India.

<sup>2</sup> Prof.S.K.Korde, Computer Department,PREC,Maharashtra,India.

## ABSTRACT

*In today's world security is the main concern in all type of applications or transactions like banking, online shopping. Remote authentication is the communication between server and client which is located at different location. In this type of system sensitive information is exchanged between two channels. In proposed system biometric image is taken as an input to a system. Then using C-PRBG keys will be generated. Using these keys chaotic encryption is done in two rounds. At the first round the output image is considered as input to the second round. This image is embedded in a video frame. There are two ways of video: one is runtime video can be captured. Second is already stored video can be taken for hiding encrypted steganographic biometric image into the frame of that video. After that it will be sent to the server for login purpose. At the server side there is all verified biometric already stored. At the server side decryption is done. The admin will verify the username with password which will be extracted from the video file. Password has a time limit; it will expire after a given time session. This system is mainly used in personnel interview, remote exam. More security is provided so this can be used in the applications which need more security. As two rounds are used for providing security to the biometric sample it leads to high security.*

**Keyword :** - Steganography, Biometric, Encryption, Authentication, Security.

## 1. INTRODUCTION

### 1.1 Authentication:

Authentication is used by a server when the server desires to know precisely who is retrieving their info. Authentication is used by a client when the client requests to know that the server is the scheme it claims to be. In authentication, the user or computer has to verify its uniqueness to the server or client. Normally, authentication by a server includes the use of a user name and password. Additional ways to verification can be done with cards, thumbprint, signature recognition, scanning of retina, vocal sound recognition, and fingerprints. Authentication by a client generally contains the server's certificate to the user in which a trusted third party is involved. Authentication does not control what responsibilities the individual can do or what files the individual can get. Authentication simply recognizes and validates who the person or system is.

### 1.2 Biometric Security:

Biometric security is connectivity continues to range across the globe, it is clear that old security methods are simply not strong enough to protect what's most important. Biometric technology is additional open than ever before, ready to bring improved security and greater accessibility to whatever needs defensive, from a door, to your car to the password on your phone. Main aim is to achieve the goals of security.

Three primary goals of Network Security are

- **Confidentiality**

- **Integrity**

- **Availability**

These three pillars of Network Security are often signified as CIA Triangle, as following.

**1.2.1 Confidentiality:** The major goal of Network Security is "Confidentiality". The function of "Confidentiality" is in defending costly business data from unauthorized persons. Entree to commercial data should be only for those individuals who of them are legitimate to use that data. Only authorize person can have access to that data.

**1.2.2 Integrity:** The additional goal of Network Security is "Integrity". Integrity objects at sustaining and promising the accuracy and consistency of data. The task of Integrity is to mark certain that the date is accurate and unfailing and is not altered by illegal individuals or hackers. The data established by the receiver must be exactly same as the data sent from the sender, without modification in even private bit of data. There is no changes in data which is received. It should be same as it is to the original data.

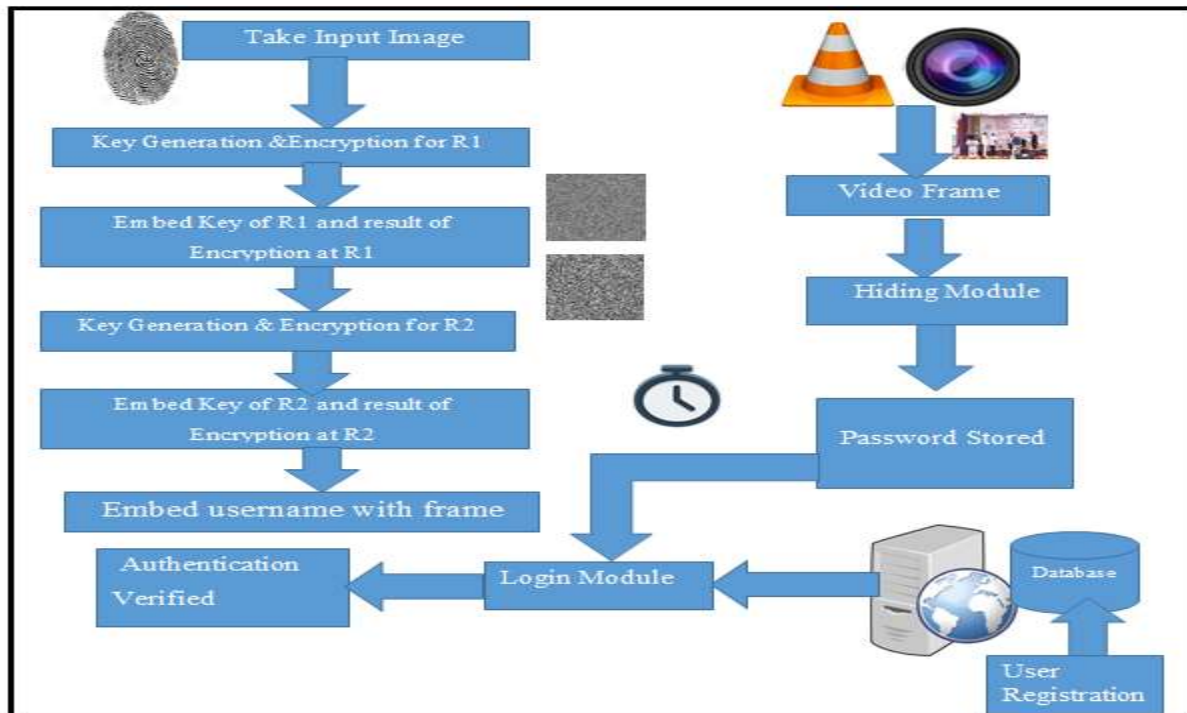
**1.2.3 Availability:** The third goal of network security is "Availability". The purpose of "Availability" in Network Security is to make sure that the Records, Network Resources or Network Services are nonstop presented to the valid users, every time they require it.

## 2. LITERATURE SERVEY:

- L. Lamport, Password authentication with insecure communication, this paper[4]proposed a remote password authentication scheme, by employing a one-way hash function. Though, in his scheme a verification table should be kept on the isolated server and if burglars interruption into it, they can adapt the table. Therefore, numerous dissimilar results have been planned, the greatest common of which is based on extended and random cryptographic keys.
- I.-E. Liao, C.-C. Lee, and M.-S. Hwang, A password authentication scheme over insecure networks, proposed a scheme that utilizes the Diffie Hellman key agreement procedure over insecure networks, [6]which permits the user and the system to decide on a session key to encrypt/decrypt their communicated letters using a symmetric cryptosystem. Random cryptographic keys are hard to remember, thus they are kept wherever and they are free centered on some substitute authentication scheme(e.g. password).
- M. Jakobsson and M. Dhiman, The benefits of understanding passwords, M. Weir, S. Aggarwal, M. Collins, and H. Stern, Testing metrics for password creation policies by attacking large sets of showing passwords, Though some passwords are simple and they can be easily predicted or cracked [9], [10]. Likewise, most individuals use the similar password across dissimilar applications; if a malicious user controls a single password, they can access multiple applications.
- Y.-y. Wang, J.-y. Liu, F.-x. Xiao, and J. Dan, A more efficient and secure dynamic id-based remote user authentication scheme, Another interesting and very promising class of remote user authentication patterns includes smart cards using dynamic users individualities per transaction section [11]. These methods aimed to overcome a common weakness of older remote authentication structures using smart cards: users identity was static in all the transaction sessions, which may escape some information about that user and can make risk of ID-theft through the message broadcast over an insecure channel.
- Klimis Ntalianis, and Nicolas Tsapatsoulis, in 2015 [1] "Remote Authentication via Biometrics: A Robust VideoObject Steganographic Mechanism over Wireless Networks. "This paper explains about how can server and client can establish communication among each other. The image is hidden in the cover image

after that this image is again encrypted and that image is embedded in video .Video will forwarded to the server as a password for verification.

### 3.ARCHITECTURE:



**Fig.1.System Architecture**

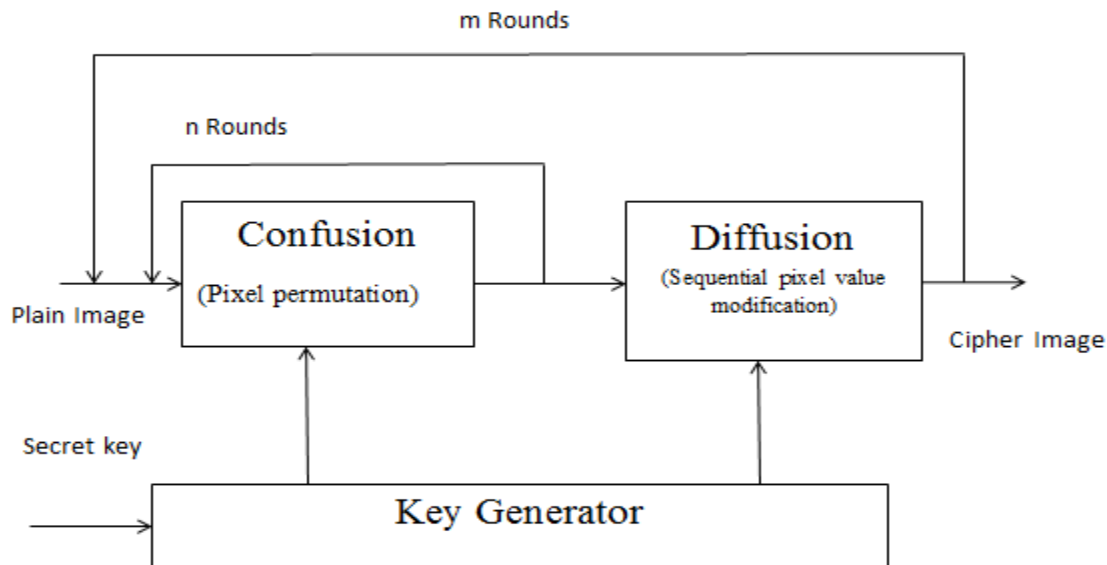
In proposed system biometric image is taken as a input. With the help of C-PRBG key will get generated. With the help of this key chaotic encryption is performed. In this encryption method initial condition and control parameters will get initialized .Encryption is done with two rounds. Result of encryption and key is hidden in frame. Username is also embedded in one frame. Similarly output image of first round is taken as input to second round .Key and result is also embedded in a frame. In next module video it may be already stored or runtime captured frames will be generated in frame this encrypted image is hidden it will pass as a password to the next module authentication module. With the help of already stored authenticated the image if verified then only allows for authentication. For all this process particular time is given for authentication process after that time password will expired.

### 4.ALGORITHMS:

#### 4.1.Chaotic Encryption-

The chaos-based image cryptosystem works in two parts[2]. The plain image is assumed at its input. The confusion stage is the pixel permutation where the position of the pixels is twisted above the entire image without upsetting the assessment of the pixels and the image becomes distorted. The pixel arrangement is accomplished by a chaotic system [1,2]. The chaotic actions is handled by the initial conditions and control parameters which are resulting from the 16-character key. To progress the safety, the second stage of the encryption method sight refining the value of each pixel in the whole image an vital tool to protect image from attackers. The basic idea of encryption[5,6] is to alter the message in the diffusion stage, the pixel values are reconstructed one by one beside the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round repeats for a

number of times to achieve a acceptable level of security. Mainly chaotic encryption is used for randomness which is more suitable for image encryption chaotic maps are used.



**Fig2. Chaotic Encryption**

So these initial conditions and control parameters act as the secret key. It is not very safe to have single the permutation stage since it may be cracked by any attack. To upgrade the security, the second stage of the encryption process aims at altering the value of each pixel in the whole image. The procedure of diffusion is also performed through a chaotic map which is mainly dependent on the initial conditions and control parameters.

In the second part i.e. diffusion part, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round reappears for a number of times to achieve a satisfactory level of security. The uncertainty property inherent in chaotic maps creates it more proper for image encryption.

#### **4.2. LSB:**

##### **4.2.1 Data embedding**

As shown in figure of LSBMR method in a and b. In fig a there is embedding stage. In the data embedding stage (Fig a.), the method first sets certain parameters, which are owned for consequent data preprocessing and region selection, and then estimates the capacity for those selected regions. If the regions are capable for hiding the given secret message  $M$ , then data hiding is carried out on the selected regions. eventually, it does some post processing to gain the stego image. Else the pattern desires to analysis the parameters, and then iterates region selection and capacity estimation until  $M$  can be embedded completely. Please note that the parameters can be changes at each time according to image content and secret message  $M$ .

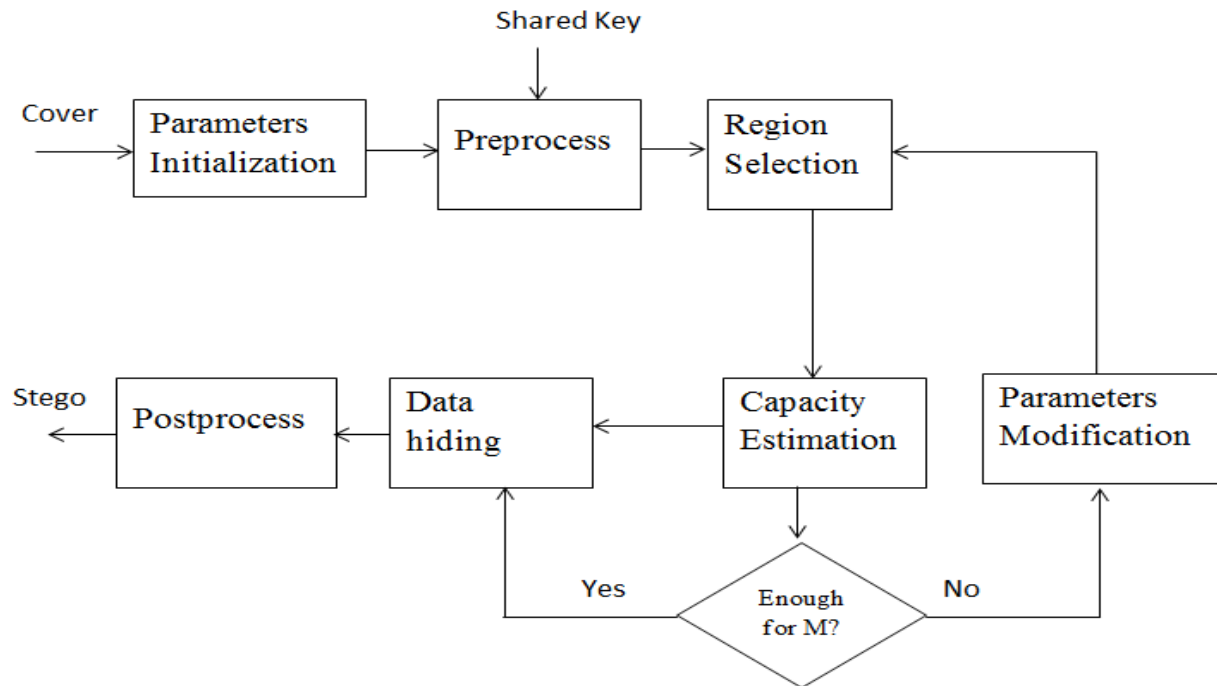


Fig 3(a) Data Embedding

4.2.2 Data extraction

The data extraction method is shown in Fig b. In this method data extraction, it firstly remove the side information from the stego image. On the basis of the side information, it perform some preprocessing and determines the regions which have been owned for data hiding. Ultimately, it gains the secret message M according to the consistent extraction algorithm.

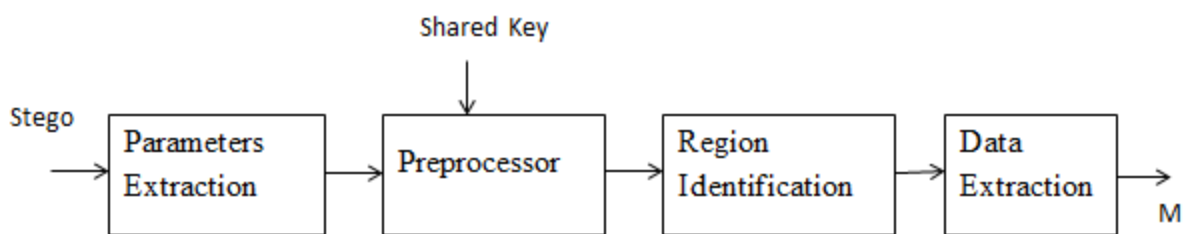


Fig 3(b) Data Extraction

• Advantages LSB Algorithm

- Security performance is high.
- Embedding capacity is large.

5.RESULTS AND DISCUSSION:

5.1.Dataset:

There are 4 images in my dataset for testing results Image1,Image2,Image3,Image4 as shown in result table in figure 5..For these images calculate PNSR values which are displayed in snapshot with the help of following formula.

$$PSNR = 10 \cdot \log_{10}(MAX^2/MSE)$$

Image	PSNR_R1(dB)	PSNR_R2(dB)
Img1	21.87	30.8
Img2	24.79	28.73
Img3	21.36	29.39
Img4	22.28	29.65

Fig 5.Result Table

**5.2.PSNR-**

Peak Signal to Noise ratio-

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs(e.g. image compression.) signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality.

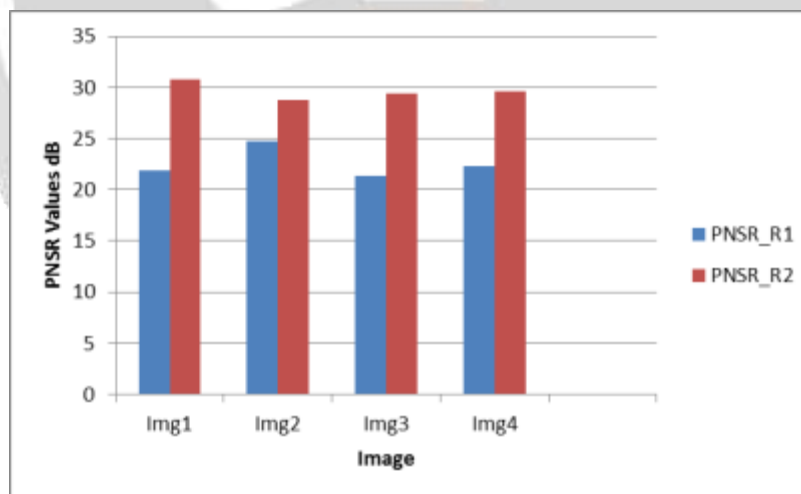


Fig.6 Result graph

Whenever we are hiding image behind cover image though PSNR ratio increased so quality is not degrading as PSNR value increasing the quality of image is also increasing. That is there is not no effect on original image which is hidden twice in a cover image. PSNR value increasing image quality also increase. In existing system there is only one round for encryption i.e image is hidden behind one image .

Consider first image img1 ,at that time of first round PSNR value is 21.37dB .After second round it increase PSNR value 30.8dB.so quality is increase though it is hidden behind cover image.

In this graph Blue color shows existing system result showing PSNR values which is less than proposed system which is shown in fig.6 with red color. In existing system there is only one round of encryption. In proposed system one more round is implemented. So the performance is high than existing system.

In this image PSNR value at first round is 24. At second round PSNR value is 28. As PSNR increases the quality of that image. This proves though image is hidden it not affects the original value.

### 5.3 Snapshot



Fig 4.Result showing PSNR Values in System

### 6.CONCLUSION:



Security is additionally significant in our standard of living, since governments as well as other administrations like school, colleges, bank etc. As they are most useful there is need of advanced authentication methods. As biometric is used as a unique identity. In this scheme biometric is used as a identity. For encryption technique is applied on biometric so it is more secure. The applications which are more confidential for those type of applications biometric security is used. This biometric signal is not as it is transmitted. It is hidden in video frame. At server side at the time of verification biometric sample is extracted from video after that it is compared with original database. Then only allowed for authentication.

### 7. REFERENCES

- [1]Klimis Ntalianis, Member, IEEE, and Nicolas Tsapatsoulis, Member, IEEE Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks in , IEEE Transactions on Emerging Topics in Computing, JANUARY 2015.
- [2]2013, Identity fraud report: Data breaches becoming a treasure trove for fraudsters, Javelin Strategy and Research, Tech. Rep., 2013.
- [3] M.-C. Chuang and M. C. Chen, An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics, Expert Systems with Applications, vol. 41, no. 4, pp.14111418, Mar.2014.

- [4]L. Lamport, Password authentication with insecure communication, Communications of the ACM, vol. 24, no. 11, pp. 770772, 1981.
- [5]D. Kundur, Y. Zhao, and P. Campisi, A steganographic framework for dual authentication and compression of high resolution imagery, in Proceedings of the IEEE International Symposium on Circuits and Systems, vol. 2. IEEE, 2004, pp. 14.
- [6]L.-E. Liao, C.-C. Lee, and M.-S. Hwang, A password authentication scheme over insecure networks, Journal of Computer and System Sciences, vol. 72, pp. 727740, 2006.
- [7]M. Weir, S. Aggarwal, M. Collins, and H. Stern, Testing metrics for password creation policies by attacking large sets of revealed passwords, in Proceedings of the 17th ACM Conference on Computer and Communications Security. ACM, 2010, pp. 162175.
- [8]Y.-y. Wang, J.-y. Liu, F.-x. Xiao, and J. Dan, A more efficient and secure dynamic id-based remote user authentication scheme, Computer Communications, vol. 32, no. 4, pp. 583585, Mar. 2009.
- [9] M. K. Khan, S.-K. Kim, and K. Alghathbar, Cryptanalysis and security enhancement of a more efficient secure dynamic id-based remote user authentication scheme, Computer Communications, vol. 34, no. 3, pp.305309, Mar. 2011.27
- [10]A. K. Das, Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards, IET Information Security, vol. 5, no. 3, pp. 145151, Sep. 2011.
- [11]P.-Y. Chen and H.-J. Lin, A dwt based approach for image steganography, International Journal of Applied Science and Engineering, vol.4(3), pp. 275290, 2006. , pp.127144.
- [12]S. Hemalatha, U. Dinesh Acharya, A. Renuka, and P. R. Kamath, A secure color image steganography in transform domain, International Journal on Cryptography and Information Security, vol. 3(1), 2013.
- [13]N. N. Rao, P. Thrimurthy, and B. R. Babu, A novel scheme for digital rights management of images using biometrics, International Journal of Computer Science and Network Security, vol. 9(3), pp. 157167, 2009
- [14]D. He, Q. Sun, and Q. Tian, A secure and robust object-based video authentication system, EURASIP Journal of Applied Signal Processing, vol. 2004, pp. 21852200, 2004.

## BIOGRAPHIES :

	<p>Miss. Manisha N. Narote received the B.E. degree in computer engineering from ZES's DCOER pune and now pursuing M.E.CSE from PREC, Loni.</p>
	<p>Prof. S.K. Korde received the B.E. degree in computer engineering from SRE'S Kopergaon and M.E. from SRMU Nanded. He is currently working as an asst. professor in PREC Loni.</p>