ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 5, May 2017

An Authentication Method Using A Verifiable Visual Cryptographic Scheme And A Steganographic Video Object Authentication Via Biometrics

Kavya. P.K, Haseena . P

***Abstract*— Remote authentication is an important requirement for secure communication. It involves the submission of encrypted information, along with visual and audio. Nevertheless, Trojan Horse and other attacks can cause serious problems, especially in cases of remote examinations or online interviewing .This system proposes an authentication mechanism based on visual cryptographic scheme and a video object steganography with biometric data .Both of these methods are combined in authentication stages and thus it improves the security of the system. The first phase is a registration with a unique image chosen by the user and a visual cryptographic mechanism is applied on that image resulting two share images. And the shares generated will be stored at receiver end and user end. Assuming that user X wants to be remotely authenticated, initially the user have to apply the share generated at the registration and by combining the both shares and verify it the preliminary authentication is done. If the verification is successfully completed then X's video object (VO) is automatically segmented. Next, one of X's biometric signals is encrypted by blowfish .Afterwards the encrypted signal is embedded in to the most significant wavelet coefficients of the video object , using its Qualified Significant Wavelet Trees (QSWTs). QSWTs provide both invisibility and significant resistance against lossy transmission and compression in wireless networks. Finally, the Inverse Discrete Wavelet Transform (IDWT) is applied to provide the stego object (SO).At the receiver end the extraction of the fingerprint and fingerprint matching process will be done using minutiae algorithm. If the fingerprints are matched then the user can successfully login to the further process.**

***IndexTerms*—Visual cryptography, Steganography, Embedding, QSWT, Blowfish, Stego object , IDWT, Fingerprint matching.**

Kavya.P.K, *Dept. of ECE, APJ Abdul kalam technological university, Jawaharlal college of engineering and technology, Palakkad, Kerala.*

Haseena.P. *Dept. of ECE, APJ Abdul kalam technological university, Jawaharlal college of engineering and technology, Palakkad, Kerala.*

I. INTRODUCTION

In digital world nowadays, the security of digital images/videos becomes more and more important since authentication is made with those digital images/videos. Authentication is the act of confirming the truth of an attribute

of a datum or entity. This might involve confirming the identity of a person or software. In this paper authentication is provided through biometric signal finger print. When using this biometric signal it's difficult to copy, forge and share . Hence the security of the biometric signal increases. Steganography mechanism is used to hide the information. Steganography is the branch of information hiding. It embeds the secret image in the cover image to hide the existence image . In early days, remote authentication is provided through password authentication methods and smart cards. While using these methods the chance of attackers to hack the password is very high. After this the remote authentication is provided through biometric signal which is more reliable and it provides three factor securities against attacks. Biometrics-based remote authentication uses fault tolerant protocols

II. LITERATURE REVIEW

A method in [5] have proposed a visual cryptography schemes to share two secret images in two shares. In the hidden two secret binary images into two random Shares, for namely A and B, such that the first secret can be seen by stacking the two shares. In multiple secrets sharing in visual cryptography described in [40] the scheme encodes a set of $n \geq 2$ secrets into two circles. The n secrets can be obtained one by one by stacking the first share and the rotated second shares with n different rotation angles this system image. In this scheme two secret images which are encoded into two shares; one secret image appears with just stacking two shares and the other secret image appears with stack two shares after reversing one of them.

A cryptography scheme for securing color image based on visual cryptography[13]. In a color image to be protected and a binary image used as key to encrypt and decrypt are taken as input data. A secret color image which needs to be communicated is decomposed into three monochromatic images based on YCbCr color space system. Then these monochromatic images are converted into binary image, in the finally the obtained binary images are encrypted using binary key image, in a called as share-l to obtain binary cipher images. To encrypt Exclusive OR operation is done between

binary key image and three half-tones of secret color image separately. In‘a verifiable visual cryptography scheme’[16] is proposed to verify whether the share is authorized, in which authors have introduced a Third Trusted Party (TTP) whose action is guaranteed. A simulation result shows that the visual quality of the obtained halftone share is observably better . A novel (2, m+1) visual cryptographic technique has been proposed image data, where m number of secret images has been encrypted based on a randomly generated master as a common share for all secrets which is decodable with any of the shares in conjunction with master share out of m + 1 generated shares. The basic concept of visual cryptography is to divide secret images into random shares. Decryption is performed by superimposing the shares. Hence the process does not require any special software or hardware device for cryptographic computations. This paper also introduces techniques of secret sharing i.e.(2, 2) secret sharing scheme, threshold secret sharing scheme and multiple secret sharing scheme. This paper also concludes that which technique will be better for secret sharing purpose. The fingerprint is the most common human biometric characteristic that has been used for personal identification. Results obtained from comparing different biometric traits show that: the fingerprint has a high value in factors like permanence, distinctiveness and performance, and medium value in universality, collectability and acceptability, while the hand-written signature has the lowest value in universality, distinctiveness, permanence and performance. For improving security, reducing fraud and enhancing user convenience, biometric systems require the process of enrolment, verification and identification. Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks proposes [22] robust remote authentication mechanism based on chaotic encryption, semantic segmentation and data hiding. This proposed human authentication scheme works over wireless channels and it provides robustness against deciphering and provides good encryption capacity.. According to the authors, the limitation of the proposed system is that Chaotic encryption is a new field for research and thus it will require a lot of time for its security mechanism to mature.

III. PROPOSED ARCHITECTURE

The purpose of this system will be to look at the use of biometrics technology to determine how secure it might be in authenticating users, and how the users job function or role would impact the authentication .In our proposed scheme we lay emphasis on biometrics to describe the authentication as in real life. Biometrics characteristics cannot be lost or forgotten and are extremely difficult to copy, share and distribute. It requires the person to be physically present as in real life at the time and point of authentication.

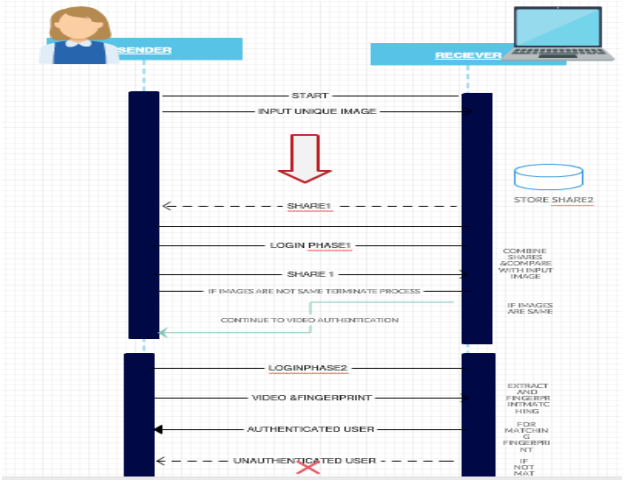

Fig.1:Sequence diagram

This kind of security can enable clients/users to use their ID and biometrics to log in to the server remotely to access their account and it provides enhanced security. We also propose to combine biometric security with steganography to enhance security over insecure channel and visual cryptographic technique at the registration phaseThe proposed scheme involves

- Apply visual cryptography to the input image and save the shares

Verify the user using share

- Extraction of the host video object from a videoconference frame and detection of the QSWTs to embed the encrypted signal,

Encryption of the fingerprint using secure force encryption

- Embedding of the encrypted signal to the host video object using steganography
- Compression of the final content and simulated noisy transmission,
- Decompression and extraction of the encrypted signal
- Verify the user by fingerprint matching

ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 5, May 2017

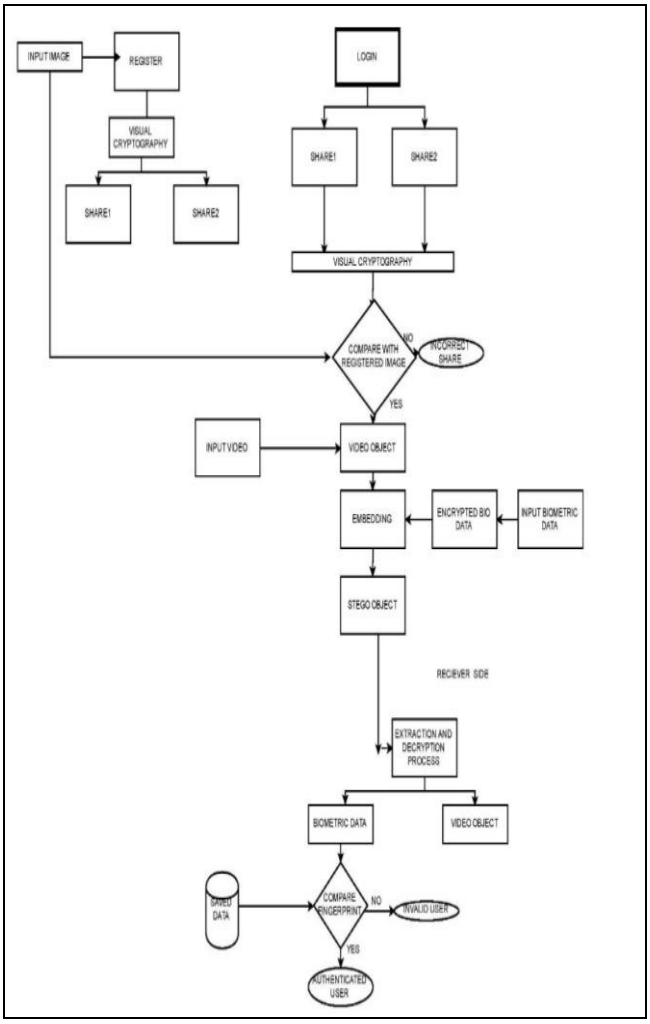

Fig 2: Overall System architecture

IV. METHODOLOGY

The proposed system is having two step authentication process to enhance the security of the system .The authentication process will be having two ends. First one is the sender/user side and second one is the receiver end where the decision of authentication will take place. The system can be divided in

- Verifiable visual cryptography
- Video object steganography
- Fingerprint verification

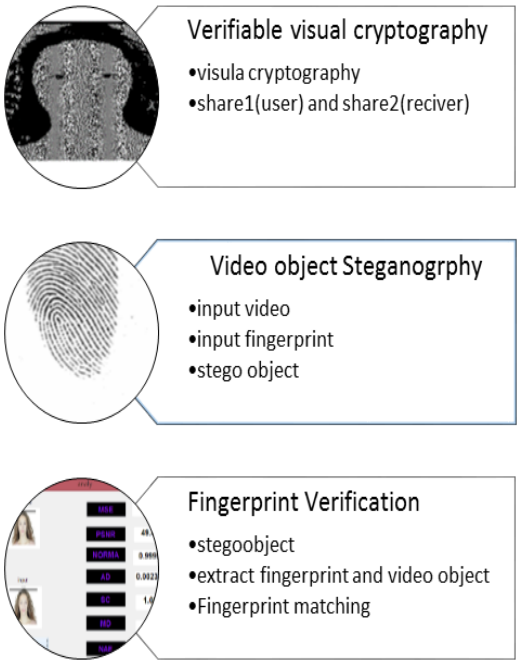

Fig 3:Flow chart

A. Verifiable visual cryptography

In this user provides the information of a person about password and a unique image selected by the user. All the information is stored in particular database. After submitting the image a visual cryptographic technique is applied to the image and two resultant shares are generated. The first share will be saved at the user end and the second share at receiver end so as to perform verification while login process.Visual cryptography is a cryptographic technique which allows visual to be encrypted in such a way that the decryption can be performed by the human visual system. Naor and Shamir[31] introduced this technique as simple and secure way of sharing secret image as password. There are two parts in this technique viz. Encryption decryption and image share generation. The encryption and decryption of message is done by simple mathematical algorithm. The second important part in this scheme is share generation of the image. Visual cryptography scheme eliminates computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography useful for the low computation load requirement.

Fig.4: Generated shares

Now the matching process after share generation ie., In this phase the reverse visual cryptographic process is done. At first the user should upload the share1 data which is created during the registration process. The share was created by applying visual cryptography on input binary image chosen

by the user. Then the receiver share is combined with the user share. The combining of both images are done by the xor operation. After getting the resultant image, It is compared with the registered image. If both the images are same then the user can go through further login process

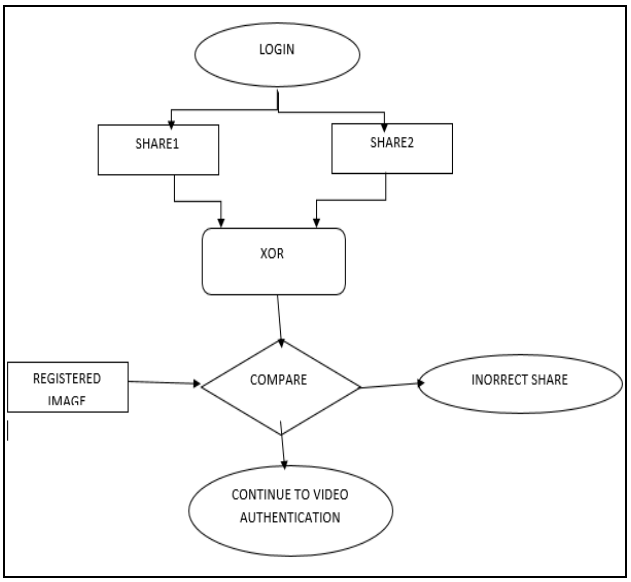

Fig.5:Share matching

B. *Video Object Steganography*

This phase of this system consist of different steps . It includes the conversion of video to different frames and select one frame to embed the biometric data. And the another step is to encrypt the biometric signal and finally embed the encrypted data to the cover image. The steps are

- Video object extraction
- Cover image generation
- Fingerprint encryption
- Fingerprint embedding in Video object

The proposed scheme involves

(a)Extraction of the host video object from a videoconference frame and detection of the QSWTs to embed the encrypted signal,

(b) Encryption of the fingerprint using secure force encryption

(c) Embedding of the encrypted signal to the host video object using steganography

(d)Compression of the final content and simulated noisy transmission

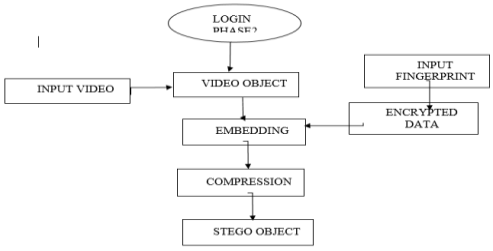

Fig 6: Stego object

V. ENCRYPTION AND STEGOOBJECT GENERATION

Image encryption is necessary for future multimedia Internet applications. Password codes to Identify individual users will likely be replaced are biometric images of fingerprints and retinal scans in the future. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper might duplicate or reroute the information. By encrypting these images, a degree of security can be achieved.

A. *Blowfish*

Blowfish is a symmetric block cipher tand it can be effectively used for encryption and safeguaring of data. It take variable-length key from 32 bits to 448 bits, for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Each line - 32 bits. Algorithm keeps two sub-key arrays: The 18-entry P-array four 256-entry S-boxes. S boxes accept 8-bit input Produce 32-bit output. One entry of P-array is used every round. After final round, each half of data block is XOR ed with one of the two remaining unused P-entries.

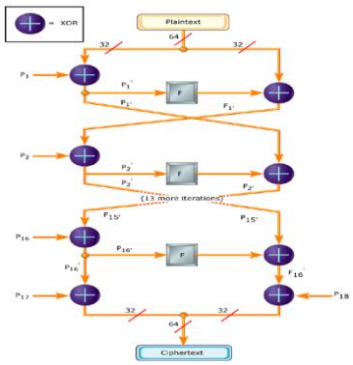

Fig.7: Blowfish

The blowfish algorithm Manipulates data in large blocks has a 64-bit block size. It has a scalable key, from 32 bits to at least 256 bits. It uses simple operations that are efficient on microprocessors. e.g., exclusive-or, addition, table lookup, modular- multiplication. It does not use variable-length shifts or bit-wise permutations, or conditional jumps. Employs pre computable sub keys. On large-memory systems, these sub keys can be pre computed for faster operation. It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.Algorithm: Blowfish Encryption

- Divide x into two 32-bit halves: xL, xR

- For i = 1to 16:
- xL = XL XOR Pi
- xR = F(XL) XOR xR
- Swap XL and xR
- Swap XL and xR (Undo the last swap.)
- xR = xR XOR P17
- xL = xL XOR P18
- Recombine xL and xR

B. Embedding

The Encrypted image is made in to vector form by vectorization . This biometric signal has to be hidden in the video object. The encrypted biometric signal is robustly hidden in the host video object. Towards this direction aim at producing a stego-video object that could protect its hidden message even in cases of compression or lossy transmission. QSWTs can play such a role, as they provide most robust solutions to data recovery, after several signal processing manipulations. In particular let us assume that the host video object has been extracted using the method described in [19]. Next the host video object is decomposed into two levels using the discrete wavelet transform .By applying the DWT once to an area of arbitrary shape,four parts of low, middle, and high frequencies, i.e., LL1, HL1, LH1, HH1, are produced. Band LL1 (HH1) includes low (high) frequency components both in horizontal and vertical direction, while the HL1 (LH1), includes high (low) frequencies in horizontal direction and low (high) frequencies in vertical direction. Sub band LL1 can be further decomposed in a similar way into four different sub bands, denoted as LL2, HL2, LH2, HH2 respectively. This process can be repeated several times, depending on the specific application. Sub bands LHN,, LH3, LH2, LH1 follow a parent-child relationship. The coefficient at the highest level is called the parent and all coefficients corresponding to the same spatial location at the lower levels of similar orientation are called children. For a given parent, the set of all coefficients at all finer scales of similar orientation corresponding to the same location are called descendants. Furthermore the wavelet coefficients can be distinguished into two types; the 'In-Node' coefficients which belong to the video object area and the 'Out-Node' coefficients which do not belong to the video object.

In the proposed steganography scheme, coefficients with local information in the sub bands are chosen as target coefficients for casting the encrypted biometric signal. Coefficients' selection is based on Qualified Significant Wavelet Trees (QSWTs) derived from the Embedded Zero tree Wavelet algorithm (EZW). In the scheme , we select the pair of sub bands that contains the highest energy content. Finally, the QSWTs are estimated for the highest energy pair of sub bands. The Hiding Strategy After selecting the pair of sub bands containing the highest energy content, [22] QSWTs are found for this pair and the encrypted biometric signal is embedded by modifying the values of the detected QSWTs. Finally the DWT is applied to the modified and an un-changed sub band to form the final stego object. So that the encrypted finger print can be embedded in to the video object securely . And thus the stego image is created and send to receiver

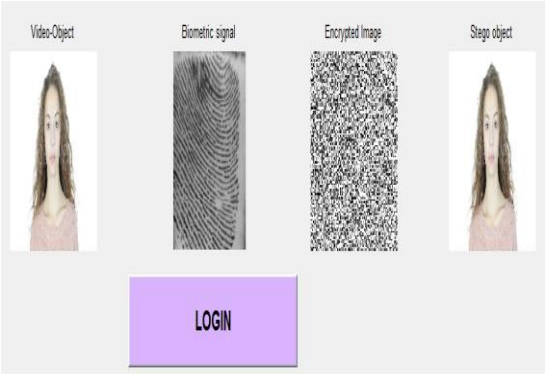

Fig.8: Stego genenerated

VI. DECRYPTION AND VERIFICATION

The input to this stage are stego object created using video object and fingerprint and the original fingerprint. Consider the Stego-object has reached the destination, the encrypted biometric signal is extracted by inverse DWT. The decryption is performed to get the hided information and original image .

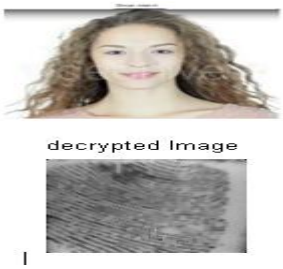

Fig.9 :Decrypted bio data

A. Deccryption

After the extraction process the finger print matching is done with the help of minutia similarities comparison. The steps for recovering the encrypted fingerprint is given below
At first the received stego-object P' and original video object P are decomposed to two levels with seven sub bands using the DWT,
Q = DWT (P)
Q'= DWT (P')
Using the size axb, the embedded positions are detected by the hiding process. The resulting hidden message coefficients are averaged and rearranged to provide the encrypted biometric signal.

B. Finger print matching

Fingerprint matching is an another step to verify the users identity. For this verification process ,require two fingerprints where first one is the reference fingerprint submitted bt the user at the registration process. And the next is the extracted fingerprint from stego video object. In this system the matching process is done using the minutiae algorithm.

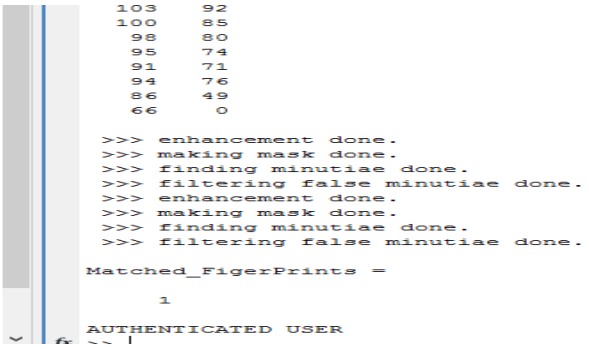

Fig.10: Fingerprint matching

VII. RESULT AND ANALYSIS

The proposed system is having three stages registration, login and verification. The main aim of this system is to authenticate a user with valid information and ensure the security of user data. The registration process generate two different share and it will act as a secret data for the further login process. This share creation is done by the visual cryptographic method. So at the login phase if these shares are combined and verify resultant image. If both are same the user can continue to video object authentication process.

Table I
Result analysis

IMAGE		Psnr	Mse	Ssm	NCER	Normalised absolute error
Finger print input	EncryptedFinger print	15.282	1926.9	0.9013	1.035	0.093
Video object	Stego object	61.97	0.04	1.0001	0.99	0.00016
Finger print Input	Decrypted finger print	40.49	5.85	0.936	1.02	0..0676

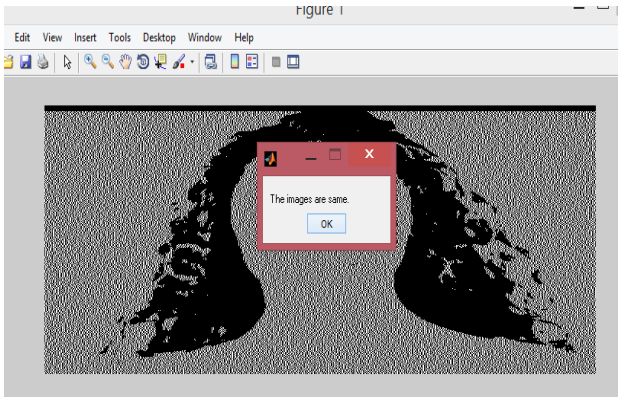

Fig.11: Share result

After the share verification the video object from the user video is extracted. Also the secret data fingerprint is encrypted using blowfish algorithm. This encrypted data is embedded on video object using QSWT .Thus the video object is created.

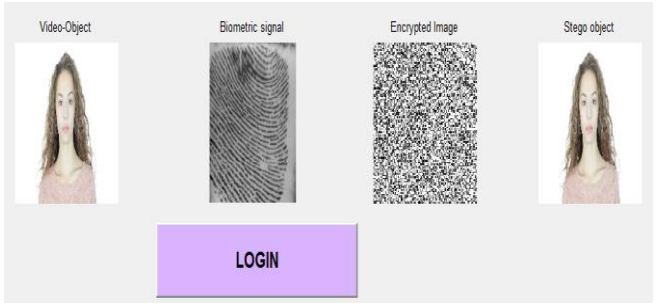

Fig.12:Login Result

At the receiver section the video object is retrieved and decompression and decryption of the image is done. The resultant image will be the fingerprint and the video object. Then the fingerprint is compared with original data and verify user is authenticated or not.

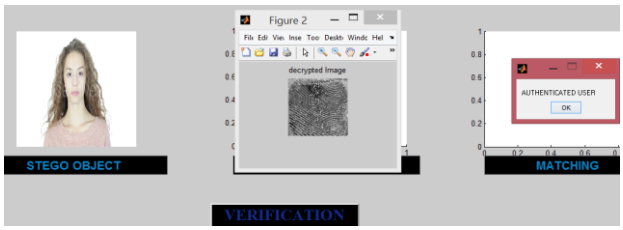

Fig.13:Verification result

B. Analysis Result

The analysis of results in different stages of the propose system is done on MATLAB software. The analyzed parameters are PSNR ,MSE, Normalised error, structural similarity ,Average difference, Maximum difference. The analysis is done between video object and stego object, input biometric signal and encrypted signal, extracted object and input object, decrypted biometric data and original data

VII CONCLUSION

In our daily lives biometrics signal plays a vital role and the development and integration of biometric authentication techniques used into practical applications increases nowadays. In this paper, we propose a robust biometrics-based authentication scheme using visual cryptography and steganography Security. If the steganography scheme is alone applied it does not ensure secrecy when it was combined with a blowfish encryption system and visual cryptographic technique it provides additional security. In this method the visual cryptographic share generation at the user registration phase and embedding biometric signal to the video object at the login phase provide a secure authentication scheme . In the proposed procedure when the images send through networks that are imperceptible to the human visual system, it also outputs a stego-object that can resist different signal distortions, and compression losses . And the Remote authentication depends up on fingerprint which is obtained from the user only. This paper presents an enhanced method to overcome the compression loss in the receiver side. Also an efficient fingerprint matching algorithm is also included to provide efficiency in authentication. This system can be further modify by replacing the biometric data fingerprint to another biometric features.

REFERENCES

[1] A. Shejul and U. L. Kulkarni, "A secure skin tone based steganography using wavelet transform," International Journal of Computer Theory and Engineering, vol. 3(1), pp. 16–22, 2011.

[2] Bailey, K. "An evaluation of image based steganography methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88,IEEE,2006.

[3] BANOCI V, BUGAR G, LEVICKY Dusan, 2011, A Novel Method of Image Steganography in DWT Domain" IEEE 2011.

[4] Behera, S.K. "Colour Guided Colour Image Steganography", Universal Journal of Computer Science and Engineering Technology, Vol. 1, No. 1, pp. 16-23, IEEE, 2010.

[5] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[6] C.-T. Li and M.-S. Hwang, "An efficient biometrics based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, vol. 33, no. 1, pp. 1–5, Jan. 2010.

[7] Chen, C-H. Ling, and M.-S. Hwang,(2014) "Weaknesses of the yoonkim-yoo remote user authentication scheme using smart cards," in Proceedings of the 2014 IEEE Workshop on Electronics, Computer and Applications. IEEE, pp. 771–774.

[8] D. He and D. Wang, "Robust biometrics-based authentication schemefor multi-server environment," IEEE Systems Journal, pp. 1–8, 2014.

[9] 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. 2185–2200, 2004.

[10] 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. 1–4.

[11] Doulamis .N.D, A. D. Doulamis, K. S. Ntalianis, and S. D. Kollias,(2003) "An efficient fully-unsupervised video object segmentation scheme using an adaptive neural network classifier architecture," IEEE Transactions on Neural Networks, vol. 14(3), pp. 616–630.

[12] Fard .M, M. R. Akbarzadeh-T, and F. Varasteh-A,(2006) "A new genetic algorithm approach for secure jpeg steganography," in Proc. of IEEE Int'l Conference on Engineering of Intelligent Systems.

[13] Gopi Krishnan S and Loganathan D,"Color Image Cryptography Scheme Based on Visual Cryptography ",Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)

[14] Gutub, A. "Pixel Indicator High Capacity Technique for RGB Image Based Steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E., pp. 154-159,IEEE,2008.

[15] Gutub, A. "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol. 2, No.1, pp. 193-198,IEEE,2010.

[16] Han Yanyan, Cheng Xiaoni, Yao Dong, He Wencai," VVCS: Verifiable Visual Cryptography Scheme", 2011 Seventh International Conference on Computational Intelligence and Security

[17] J. Dong and T. T., "Security enhancement of biometrics, cryptography and data hiding by their combinations," in Proceedings of the 5th International Conference on Visual Information Engineering. VIE 2008, 2008, pp. 239–244.

[18] Transactions on Emerging topics on computing.

[19] Kaur B, Kaur A, Singh J, 2011,"Steganographic approach for hiding image in dct domain",IJAET, Vol 1, Issue 3.

[20] Kelash H.M, Abdel wahab O.F, Elshakankiry ,Etsayed H.S, 2013, „Hiding Data in videoSequences Using Steganography Algorithms" IEEE.2013

[21] Klimis Ntalianis and Nicolas Tsapatsoulis (2015), "Remote Authentication Via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks" in IEEE Transactions on Emerging topics on computing.

[22] Kumar S, Latha M, 2014, "DCT Based Secret Image Hiding in video sequence" IJERA,2014

[23] Li .S, X. Zheng, X. Mou, and Y. Cai, (2002,) "Chaotic encryption scheme for real-time digital

video," in Proceedings of Real-Time Imaging VI, vol. 4666. SPIE, pp. 149–160.

[24] Majumder J, Mangal S, 2012, „An Overview of image steganography using LSB Technique",IJCA.

[25] Marwaha, P. "Visual cryptographic steganography in images", Second International conference on Computing, Communication and Networking Technologies, pp. 34-39, IEEE, 2010.

[26] Moon S.K, Raut R.d, 2013,"Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security", IEEE.

[27] Mrs. A. Vinodhini, M. Premchand, M. Natarajan "Visual Cryptog-raphy Using Two Factor Biometric system for Trust Worthy Authentica-tion", IJSRP 2012, vol. 2, Issue 3.

[28] Murdoch .S, M. Bond, and R. J. Anderson,(Nov 2012) "How certification systems fail: Lessons from the ware report," IEEE Security and Privacy, vol. 10, no. 6, pp. 40–44.

[29] N. Askari, C. Moloney, H. M. Heys "Application of Visual Cryptog-raphy to Biometric Authentication", Newfoundland Electrical and Com-puter Engineering conference, 2011

[30] N. N. Rao, P. Thrimurthy, and B. R. Babu, "A novel scheme for digita rights management of images using biometrics," International Journal of Computer Science and Network Security, vol. 9(3), pp. 157–167, 2009.

[31] Noar M., Shamir A., 1995. Visual cryptography. Advances in Cryptog-raphy. Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, Spring-er-Verlag. 1 – 12.

Kavya PK is M. tech final year student of Applied electronics and Communication system from Jawaharlal college of engineering and Technology, Palakkad affiliated to APJ Abdul Kalam Technological University. Her current research interest is Steganography and Cryptography. She received her B. Tech in Electronics and Communication Engineering from Ammini college of Engineering,Palakkad affiliated to Calicut university.

Haseena P is Assistant Professor at Department of electronics and Communication Engineering, at Jawaharlal college of engineering and Technology, Palakkad affiliated to APJ Abdul Kalam Technological University.. She has teaching experience of more than 3 years to graduate and postgraduates. She received her M. Tech in Electronics and Communication Engineering from Adhiyamaan college of engineering, hosur, india. She received her B. Tech in Electronics and Communication Engineering from College of Engineering Poonjar, Kottayam.