DOI: http://doi.org/10.32792/utq.jceps.12.01.09

Hiding fingerprints in facial features using DCT

Zahraa qasim **Prof. Dr. Kadhim Al ibraheemi**

1, 2Computer Science Department, College of Education for Pure Science, Thi- Qar University
Nassiriya, Iraq.

Received 1/3/2022 Accepted 22/3/2022 Published 30/3/2022

Abstract:

The need to use a biometric authentication systems in many applications because we need to provide adequate protection for the sensitive personal data that the systems deal with increases to prevent potential attacks that could harm the widespread use of biometric systems.

The goal of this research is to provide a high level of biometric data security for a face and ten fingerprint biometric system. All cloaking techniques that deal with the face image hide the fingerprint data at the image level and produce a stego-image. The researcher proposes a new methodology to hide the data of ten fingerprints in templates .The face is at the feature level rather than the image level.And also a new encryption algorithm based on the idea of MESR combined with DCT to encrypt the details of the fingerprint before hiding it. As a result, alternative methods such as encryption are required to safeguard the features, which necessitates the creation of extra accounts .The researcher proposes the following solutions to alleviate these disadvantages Where the output was extracted using the proposed method of DCT(Discrete cosine transform) and MESR(maximally stable extremal regions) to hide fingerprints in the features of the face, as well as used the proposed method for de-masking using IDCT, and the results were 100% identical when de-hiding.

Keywords:
face recognition, Steganography , face features, minutiae finger print ,DCT.

1. Introduction

Biometric authentication became a typical feature in smartphones and other mobile devices. It is a popular and dependable access control technique[1]. Some technologies, like any multifactor authentication technology, necessitate this same secure storage of biometric features in a digital database for later multi - biometric matching [2]. To preserve secrecy, any classified data must be stored using safe encryption. Data hiding is a technique that can be used. improve the protection of the biometric during the transfer of encrypted data, an authentication method is image, that may or may not be associated to the subject being authenticated[3]. Cyber thieves can utilize biometric data, just like any other person's personal information, to perpetrate identity theft, and its monetary value makes it a commodity that can be traded on dark web marketplaces. The dark web is a collection of websites that can only be accessed through specific browsers that have anonymizing features to help users avoid being identified. [4]. According to the most recent data available on the dark web, the worth of stolen personal information ranges from around$5 for a credit card to more than $1000 for a person's whole medical history[5]. Theft of biometric data allows a cyber-criminal to carry out replay or substitution attacks, getting access to a huge amount of personal information such as social security numbers and credit card details. debit card numbers, driver's license numbers, and passport numbers are all examples of personal information. As a result, all safeguards that strengthen the security of a person's sensitive data must be employed. The defence-in-depth information security paradigm uses overlapping multiple controls to assure security when one layer of protection fails [6].

2. Related Works

Some few research papers on information security in MANETs (Mobile ad hoc Networks), as well as various biometric security techniques and multimodal biometrics, are briefly discussed below.

Xiao. (2004) [7] proposed a new technique for mobile user authentication. Each group has a cryptographic key that is used for internal communication. Each group member has a profile that contains all of the ID holders' information, and the group leader keeps track of the group members' biometric templates. The group leaders operated as dispersed authenticators instead of a central authentication server. However, this system solely employed fingerprints for authentication, and if one was compromised, the entire connection would be compromised as well. Additionally, uni-modal biometric systems have a number of drawbacks.

Kwon. T and Moon. H. (2008) [8] proposed an authentication methodology that combines multimodal biometrics and cryptographic mechanisms for border control applications.

Sasidhar, et al. (2010) [9] The used state-of-the-art Commercial Off-The-Shelf items to test the accuracy and performance of multimodal biometric authentication systems. To get over the drawbacks of uni-modal biometrics.

Jagadeesan , et al. (2010) [10] For safeguarding the entire communication between users, a cost-effective technique based on multimodal biometrics (Iris and Fingerprint) was proposed. Authentication is not implemented in this system at the same time. Because authentication is critical in mobile ad hoc networks.

Masoud Afrakhteh and Subariah Ibrahim. (2010) [11] developed an Improved Least Significant Bit Scheme that is resistant to the Chi-Squared attack. There is a difficult challenge with steganographic techniques, notably in the traditional least significant bit (LSB) insertion approach, which is how to embed desired secret bits in a cover medium in a way that is not visible to human vision. Unlike BPCS(Business Planning and Control System), PVD(Peripheral vascular disease), and MBNS(Bachelor of Medicine, Bachelor of Surgery), which employ 3 or 4 immediate neighbors of each pixel, this work provides a method that uses more surrounding pixels, and it is eventually proven that the method is resilient against Chi-squared assault.

Guo-Shiang Lin, et al. (2010)[12] a framework for Enhancing Based on the Simulated Annealing Algorithm, image steganography with picture quality optimization and anti-steg analysis is possible. This paper proposes a closed-loop computing framework that iteratively searches for proper pixel/coefficient modifications to improve a base steganographic scheme with improved picture quality and anti-steg analysis capability.

Alok Kumar Vishwakarma1 and Atul Kumar. (2011) [13] Biometrics in Combination with an Elliptic Curve Crypto-Stegano Scheme was offered as a Novel Approach for Secure Mobile Voting. This paper explains how to use cryptography and steganography to create a safe mobile voting system.

Nabin Ghoshal and J. K. Mandal.(2011) [14] proposed a Authentication of Color Images Using a Steganographic Scheme This study describes a new steganographic technique that uses the Discrete Fourier Transform to provide color image authentication in the frequency domain (DFT). This approach outperforms discrete cosine transformation (DCT), Quaternion Fourier Transformation (QFT), and Spatio Chromatic DFT (SCDFT)-based algorithms, according to experimental results.

Ali Hussein Jazi .(2018) [15] Providing a high level of security for biometric data for a biometric system that uses a face image and one fingerprint. One of the disadvantages of this method is that the data is saved in the face template.

3. Problem Statement

Biometric data is considered sensitive data, and its storage in databases or transmission over the Internet may lead to theft and use in unlicensed systems. For this purpose, to maintain the integrity of the biometric data, , Biometric techniques have advanced fast over the last decade and are now employed in a variety of settings, including banking and government agencies, retail sales, law enforcement, health care, and airport/border controls. Biometric data security and integrity is a huge concern, as many of the benefits of biometrics can easily become a hindrance. As a result, in order to promote the widespread use of biometric techniques, the need to protect biometric data, particularly fingerprint data, becomes critical. An unauthorized person can gain access to a system by using latent fingerprints. People leave latent prints when they touch hard surfaces, making it easy to gather a latent fingerprint. If a latent print was successfully recovered by an unauthorized user, This may allow him or her to get access to the system, putting user's privacy at risk. Stolen data can also be used for unlawful purposes like identity theft, forgeries, or fraud. As a result, improved data security is vital.

4.Proposed Method

The Proposed technique for multiple biometric-based authentication steganography and all its parts are explained. This technique is consist of two parts (registration and steganography part and D-steganography and Verification part). Figure (1) shows stages of registration and steganography part

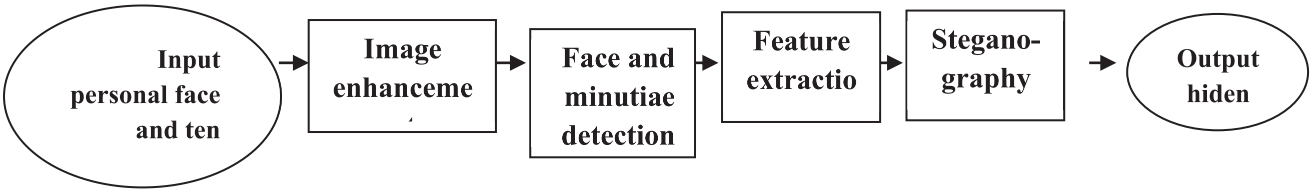
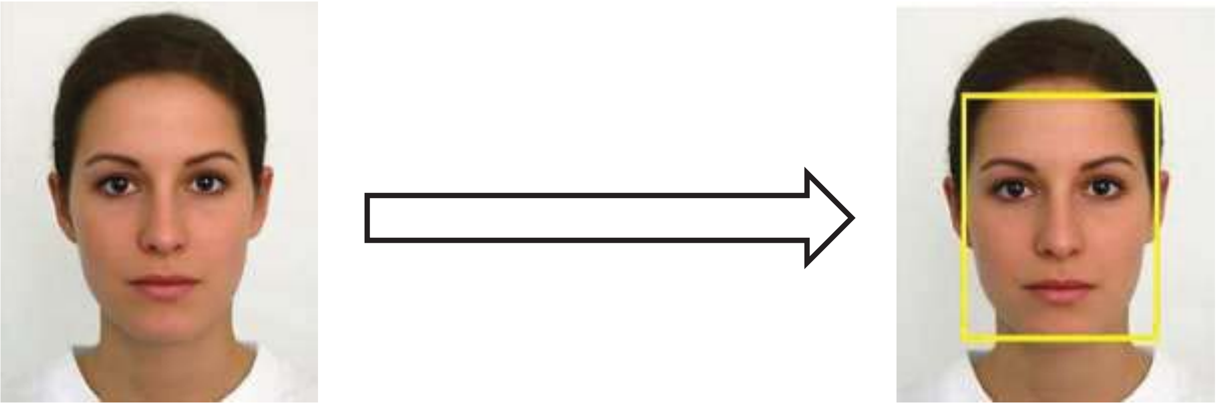


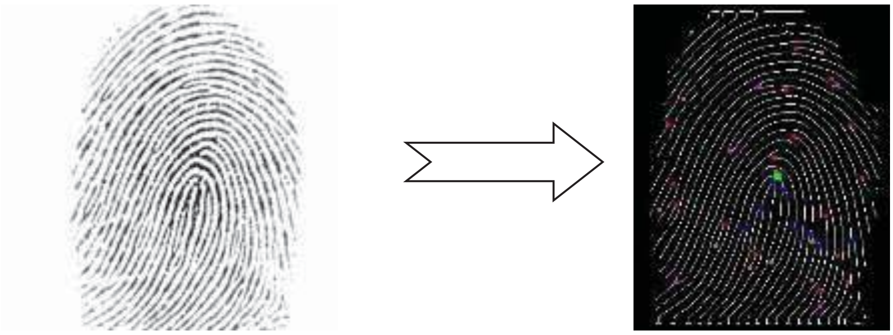
Figure (1): registration and steganography part.

The person’s image is captured by the camera and the ten fingerprints are taken by the scanner and they are entered into the system .The Viola-Jones algorithm will be applied to the person's image for the purpose of face detection , the MSER algorithm will be applied to the image of the detected face for the purpose of extracting the facial features. After that, the minutiae is discovered from the images of the finger prints and its features are extracted according to "Fingerprint Matching using A Hybrid Shape and Orientation Descriptor" method. After the face and finger prints are ready, by using the DCT the ten finger prints features will be hidden in the face features and stored as a data file. Figure (2) shows person’s image before and after applying Viola-Jones algorithm.



Figure(2) : person’s image before and after applying Viola-Jones algorithm

Figure (3) shows detected minutiae before and after applying "Fingerprint Matching using A Hybrid Shape and Orientation Descriptor" method.



Figure(3) : person’s image before and after minutiae detection

4-1 Feature extraction

After the face image is detected, the MSER algorithm will be applied for the purpose of extracting the facial features Figure (4) shows extracted facial features.

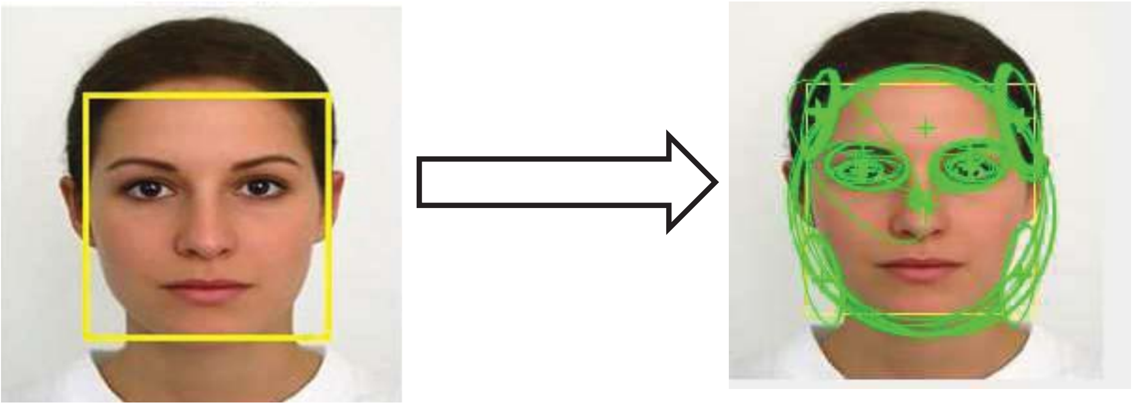


Figure (4) shows extracted facial features

Each minutia in the template and test fingerprints has an extended triplet structure defined as a 2-neighbourhood structure in the form of x, y, r1, 1, r2, 2, where r1 and 1 are the polar co-ordinates of the closest minutia, and likewise for the second closest minutia, r2 and 2 are the polar co-ordinates of the second closest minutia…

This process is repeated ten times to hide the features of ten fingerprints in the facial features, where each time we take six elements from each cell of pixel list array and repeat the same previous steps In order to create a serious matrix, six elements will be cut out from each cell as shown in the algorithm, and then the fingerprints will be hidden in the new matrix and the variable value added 'g'. Cells containing less than 60 elements will be discarded and not entered into the steganography process (Because according to the condition, we extract a new matrix through the cells resulting from the facial manifold whose contents of cells are more than 60 or less and are neglected)Algorithm(1).

Algorithm(1) proposed Steganography

Input:

Input face feature (pixel list array) Ai, and ten matrix of minutiae features Bi, g=0.000001.

Output:

New pixel list array after Steganography

Start

1. For i=1:10
2. Take 6 elements from every vector of pixel list to build a new 2D matrix and Apply DCT on it (USE: 2.5.3).

$$F(u,v) = \frac{2C(u)C(v)}{N}\sum_{i=1}^{N}\sum_{j=1}^{N} f(i,j)\, cos\left(\frac{(2i-1)(u-1)\pi}{2N}\right) cos\left(\frac{(2j-1)(v-1)\pi}{2N}\right)$$

$$= \frac{2C(u)C(v)}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\, cos\left(\frac{(2i+1)u\pi}{2N}\right) cos\left(\frac{(2j+1)v\pi}{2N}\right)$$

$$where 0 \le i, v \le N - 1 and C(n) = \begin{cases} \frac{1}{\sqrt{2}} & (n = 0) \\ 1 & (n \neq 0) \end{cases}$$

3. Multiplying the Matrix of the minutiae features(i) by g(to reduce noise)
   Bi=Bi*g
4. Add two matrixes ; Ri = rows number of minutiae features matrix.
   Ri=Ai+Bi
5. Re-transform the product matrix. using equations (Dct)

```
    6. Dismantling the produced array and returning the elements to their old positions in the pixel
       list array and insert r to it.
    7. End for loop
    8. Save new pixel list array as data file
End
```

4.2 D-steganography

Most of the D-steganography steps are the reverse steps of steganography and in this stage the input is the new pixel list array after Steganography, initially, the vector r is truncated from pixel list array Which contains the number of rows for ten matrices of the minutiae features.

The new pixel list array is then copied, To get the original pixel list array, the copy of new pixels list array are changed from double to integer by rounding its elements to the nearest integer number. And by this method, facial features are restored. Then two 2D matrixes are built from the new pixel list array and the original pixel list array By taking 6 elements from each cell to form two 2D matrixes, and transformed them by using IDCT and get the absolute value of their subtraction product and the matrix elements produced from the previous step are divided by the same small value that was multiplied by the minutiae features matrix during steganography. To get the matrix of minutiae features the first rows of the matrix produced from the previous step are truncated by numbers of rows (r). Algorithm(2) shows proposed D-Steganography algorithm steps.

```
Algorithm( 2) D-Steganography

Input:
New pixel list array after Steganography Ri ,g=0.000001.
Output:
face feature (original pixel list array) and ten matrix of minutiae features.
    1. Cut r vector to get number of rows of ten matrix of minutiae features.
    2. Copy new pixels list array.
Ci=Ri
    3. To get the original pixel list array, the copy of new pixels list array are changed from double to
       integer by rounding its elements to the nearest integer number. And by this method, facial
       features are restored.
Ri=int(Ri)
    4. For i=1:10
    5. Reconstructing two matrices from the new pixel list array and the original pixel list array By
       taking 6 elements from each cell to form two 2D matrixes, the number of columns in them is 6
```

.

6. transform the two 2D matrixes using DCT and get the absolute value of their subtraction product.

$$F(u,v) = \frac{2C(u)C(v)}{N}\sum_{i=1}^{N}\sum_{j=1}^{N} f(i,j)\cos\left(\frac{(2i-1)(u-1)\pi}{2N}\right)\cos\left(\frac{(2j-1)(v-1)\pi}{2N}\right)$$

$$= \frac{2C(u)C(v)}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\cos\left(\frac{(2i+1)u\pi}{2N}\right)\cos\left(\frac{(2j+1)v\pi}{2N}\right)$$

$$where 0 \le i,v \le N-1 and C(n) = \begin{cases} \frac{1}{\sqrt{2}} & (n=0) \\ 1 & (n \neq 0) \end{cases}$$

7. The matrix elements produced from the previous step are divided by the same small value that was multiplied by the minutiae features matrix during steganography.
8. Retransform produced matrix from the previous step (IDCT)[16]

$$F(i,j) = \frac{1}{4}\sum_{i=0}^{7}\sum_{J=0}^{7} C_U\ C_V\ F(U,V)COS\left(\frac{(2i+1)U\pi}{16}\right)COS\left(\frac{(2j+1)V\pi}{16}\right)$$

9. To get the matrix of minutiae features (i), the first rows of the matrix produced from the previous step are truncated by r(i) rows.
10. Save matrix of minutiae features (i).
11. End for loop.

12.End algorithm

4.3.Comparing the proposed system with other studies

In this section, the proposed system will be compared with the previous study submitted by researcher Ali Hussain Jazea, entitled (“An improved scheme for multi-biomitric Athentication”).[15]

1- In the proposed system, the minutiae features is hidden for ten fingers in the facial features, while the previous study is hidden the minutiae features for one finger in the facial features.
2- In the proposed system, the original data is not preserved and the facial features and the minutiae features are retrieved from the output file, while in the previous study the original data is kept because they need it to retrieve the minutiae features.
3- In the proposed system, the DCT is used for the purpose of hiding the data and taking advantage of the feature of the spread of the data included in the whole of the original data, while the xor is used in the previous study.
4- In the proposed system, the data is retrieved without any error or loss, while in the previous study there are errors.

5.Implementation Results:

The proposed steganography technique was applied on set of hundred different fingerprint images files for ten persons by different small value as(g1=0.0001, g2=0.00001, g3=0.000001) and the table (4) shows that the best results was by 0.000001,Measures that were used are Peak signal-to-noise ratio (PSNR), Normalized Cross Correlation(NCC) and mean squared error (MSE) and the False Acceptance Rate (FAR), False Rejection Rate (FRR).

This technique was applied using a Lenovo laptop with a Core i7 2.7 GHz Lenovo Core i7 2.7 GHz processor 8GB RAM and 64-bit operating system 8GB
MATLAB 2020 B.

Table (1) g1 =0.0001;

ID	PSNR	NCC	MSE
1	62.882	1	5.1498e-07
2	62.915	1	5.1111e-07
3	63.853	1	4.118e-07
4	59.649	1	1.0843e-06
5	56.157	1	2.4226e-06
6	60.812	1	8.2945e-07
7	59.844	1	1.0366e-06
8	56.664	1	2.1558e-06
9	62.08	1	6.1945e-07
10	61.87	1	6.5009e-07
Average	60.673	1	1.0236e-06

Table (2) g2 =0.00001;

ID	PSNR	NCC	MSE
1	82.882	1	5.1498e-09
2	82.915	1	5.1111e-09
3	83.853	1	4.118e-09
4	79.649	1	1.0843e-08
5	76.157	1	2.4226e-08

6	80.812	1	8.2945e-09
7	79.844	1	1.0366e-08
8	76.664	1	2.1558e-08
9	82.08	1	6.1945e-09
10	81.87	1	6.5009e-09
Average	80.673	1	1.0236e-08

Table (3) g3 =0.000001;

ID	PSNR	NCC	MSE
1	102.88	1	5.1498e-11
2	102.91	1	5.1111e-11
3	103.85	1	4.118e-11
4	99.649	1	1.0843e-10
5	96.157	1	2.4226e-10
6	100.81	1	8.2945e-11
7	99.844	1	1.0366e-10
8	96.664	1	2.1558e-10
9	102.08	1	6.1945e-11
10	101.87	1	6.5009e-11
Average	100.67	1	1.0236e-10

The time was calculated to perform the Steganography and D-Steganography process .Table (4) shows the Steganography time and D-Steganography time.

Table (4) Steganography time and D-Steganography time.

ID	Steganography time(second)	D-Steganography time(second)
1	0.0261	0.0203
2	0.0250	0.0123
3	0.0313	0.0334
4	0.0348	0.0291
5	0.0182	0.0107

6	0.0233	0.0112
7	0.0186	0.0104
8	0.0181	0.0106
9	0.0208	0.0109
10	0.0185	0.0096

6.Conclusion:

can use this technology to provide a high level of preservation of biometric data. The metric system uses an image of one face and ten fingerprints .The ten fingers use, the result will be better than one finger in the case of one finger in general is exposed to burns, wounds or cuts (finger amputation), so the system will object, therefore, if they use ten fingerprints, there are nine other fingers that show the result if it happens One finger damage, and it will add more security and reliability to the system. Using one part of the facial features or one area to hide ten fingerprints will affect the face template or vulnerabilities, and therefore we hid ten fingerprints in different areas of the facial features according to the study we conducted .It has been determined who is the person authorized to use the trusted system is more secure and therefore only people who have any fingerprints that access the face are entitled to enter the system.The method that we used is safe, it was used because it does not retain the information to retrieve or extract the original data, neither for features , meaning one file is the storage file itself, from which we extract the original minutiae or features. The small value 'g' must be a small value so that the results are 100% identical after decoding or decoding steganography .This is a new and modern method that has not been used before without storing one of the original data.

7.References:

[1] Meng, W.; Wong, D.S.; Furnell, S.; Zhou, J. Surveying the development of biometric user authentication on mobile phones. IEEE Commun. Surv. Tutor. 2015, 17, 1268–1293.

[2] Campisi, P. Security and Privacy in Biometrics; Springer: Berlin/Heidelberg, Germany, 2013; Volume 24.

[3] Marqués, I.; Grana, M. Image security and biometrics: A review. In International Conference on Hybrid Artificial Intelligence Systems; Springer: Berlin/Heidelberg, Germany, 2012; pp. 436–447.

[4] Sirull, E. What Is the Dark Web? 2018. (accessed on 11 May 2018).

[5] Stack, B. Here'S How Much Your Personal Information Is Selling for on The Dark Web. 2018. (accessed on 11 May 2018).

[6] Hillman, S. Physical security 101: Evolving 'defense in depth'. InTech Magazine, May/June 2011.

[7] Xiao, Q., 2004. A biometric authentication approach for high security ad-hoc networks. Proceedings of the 5th Annual IEEE SMC Information Assurance Workshop, Jun. 10-11, IEEE Xplore Press, pp: 250-256. DOI: 10.1109/IAW.2004.1437824.

[8] Kwon, T. and H. Moon, 2008. Biometric authentication for border control applications. IEEE Trans. Knowl. Data Eng., 20: 1091-1096. DOI: 10.1109/TKDE.2007.190716.

[9] Sasidhar, K., V.L. Kakulapati, K. Ramakrishna and K.K. Rao, 2010. Multimodal biometric systems-study to improve accuracy and performance. Int. J. Comput. Sci. Eng. Survey, 1: 54-61. DOI: 10.5121/ijcses.2010.1205.

[10] Jagadeesan, A., T. Thillaikkarasi and K. Duraiswamy, 2010. Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature. Int. J. Comput. Appli., 2: 975-8887.

[11] Guo-Shiang Lin, Yi-Ting Chang, and Wen-Nung Lie “A Framework of Enhancing Image Steganography with Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm” IEEE Transactions on Multimedia, August 2010.

[12] Masoud Afrakhteh and Subariah Ibrahim “Enhanced Least Significant Bit Scheme Robust Against Chi-Squared Attack” Fourth Asia International Conference on Mathematical/Analytical Modeling and Computer Simulation 2010.

[13] Alok Kumar Vishwakarma1 and Atul Kumar “A Novel Approach for Secure MobileVoting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme” International Journal of Technology and Engineering Systems, March 2011.

[14] Nabin Ghoshal, J. K. Mandal “A Steganographic Scheme for Colour Image Authentication (SSCIA)” IEEE-International Conference on Recent Trends in Information Technology, June 3-5, 2011.

[15] Ali Hussein Jazi.”An improved scheme for multi-biomtric authentication”2018.

[16] ITU-T Recommendation H.263, "Video Coding for Low Bit-Rate Communications," Telecommunication Standardization Sector of ITU (03/96)(2012).