

A Hybrid Secure Architecture for Passport Verification system using Visual Cryptography and Steganography

P. Vijayakumar¹, R. Rajashree²

1. Assistant Professor (Sr.), VIT University, Chennai, India

2. Assistant Professor, GKM College of Engineering & Technology, Chennai

*Corresponding author E.mail: 1vijayrgcet@gmail.com; rajashree.ece@gmail.com

ABSTRACT

The privacy is the main concern in the present days and especially in biometrics verification of passport using individual's personal data. Many researchers have put forward various solutions for biometric verification system. The existing visual cryptographic scheme for biometric verification system provides security to the face image present in the biometric template during the storage and transmission of data. The proposed hybrid architecture employs the advantages of visual cryptography and steganography for passport verification. It extends the privacy to the image as well as the personal information with less communication complexity. It also provides greater level of security.

Keywords: Biometrics, Visual cryptography, Face images, Steganography, Passport verification system, Communication complexity, Elliptic Curve Cryptography.

INTRODUCTION

Biometrics is the science used for individual's authentication and identification based on physiological and behavioural traits such as fingerprints, audio, gait, iris patterns, hand geometry, images. In biometric system, the raw biometric data is stored in template and the extracted features set is compared with the template stored in the database for identification. Visual cryptography (VC) is a secret sharing scheme that uses encryption and decryption process using mathematical computations. The encrypted message can be decrypted only by the intended receiver. VC scheme proposed by Naor and Shamir serves as a basic model and has been applied to many applications. In visual cryptography is explained in, prescribed secret image is taken as an input which is split into two shared images that do not reveal any information. The secret image is reconstructed by overlapping or stacking of shared images. The usage of Steganography is the technique of hiding information that makes the detection of hidden messages difficult. The information or messages is hidden in images in such a manner that any change made to the image is barely visible. Least significant bit (LSB) insertion is a simple approach to hide information in image file. This simplest steganography technique embeds the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. This paper is structured in the following way: Related works for security enhancement of biometrics system, visual cryptography and steganography schemes are discussed in section 2. Section 3 presents the existing system. Section 4 presents the proposed system, experiments and results are shown in section 5 and section 6 concludes the paper.

Existing Passport Verification System: The input private image is decomposed into two independent sheet images that are stored in two different database servers such that the private image can be reconstructed only when both sheets are simultaneously available. The existing architecture stated is fails in extending the privacy to the personal information of an individual. The working of the existing system to store and de-identify an image is shown in the figure 1.

Proposed Passport Verification System: The plain text which includes the details regarding the individual is converted into cipher text the encrypted data is then hidden in an image using steganography. This input private image is now decomposed into two independent sheet images that are stored in two different database servers. The private image can be reconstructed only when both sheets are simultaneously available from both the data base servers. The reconstruction is performed by overlapping the two shared images available in the database. The data is extracted by decryption of cipher text into plain text. The passport verification is done by matching the details provided by the individual with the details enrolled in the database. This system extends the privacy to the image as well as the personal information.

Embedding system: These points are encrypted using Elliptic Curve Cryptographic encryption algorithm to obtain the cipher text point. These ciphertext points are embedded into personal image using steganography – LSB algorithm. The resultant stego image is given as input to visual cryptography technique where two shared image IM1 and IM2 are used to hide the stego image. These shared images are stored in two different servers as shown in Fig.2 and Fig.3.

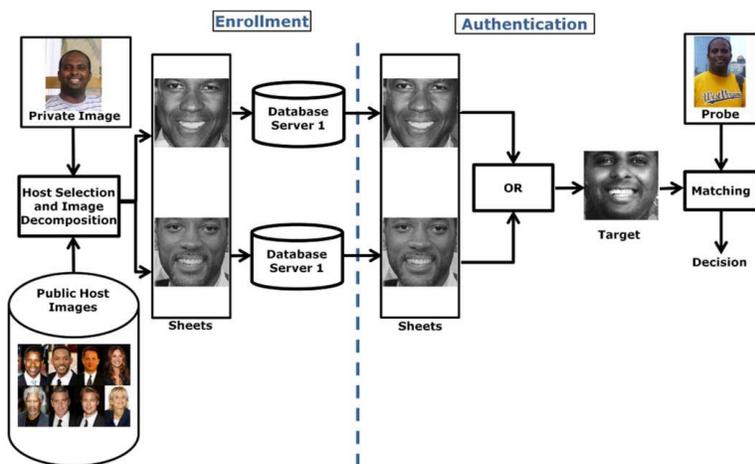


Fig.1. Existing approach for de-identifying and storing a face image.

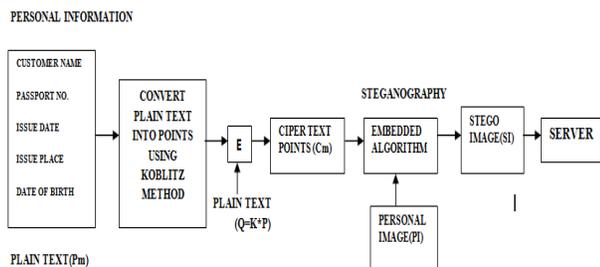


Fig.2. Hiding personal information into image using steganography

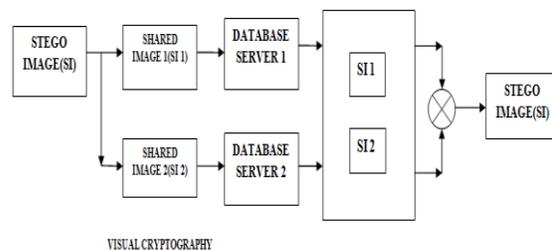


Fig.3. Split stego image into two share image 1 and image 2 using Visual cryptography

Verification System: During passport verification, customer personal information and image are verified as shown in fig.4. Before going to extract the personal information's and image, first step is to overlap the two share images from two different servers to obtain stego image. This stego image is given as input to extraction algorithm to get personal information in the form of cipher text C_m from stego image. This ciphertext points are decrypted using ECC decryption algorithm to get plaintext points. These plaintext points are converted into plaintext message using Koblitz method. These plaintext messages are compared with passport detail of the user. If passport details are matched with recovered plaintext information, then user is accepted or rejected to get service. The working of the proposed system to store and de-identify an image and personal information of an individual is shown in the Fig. 5.

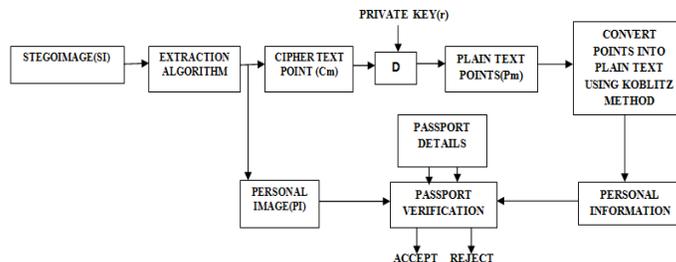


Fig.4. Retrieving the personal information and image using ECC

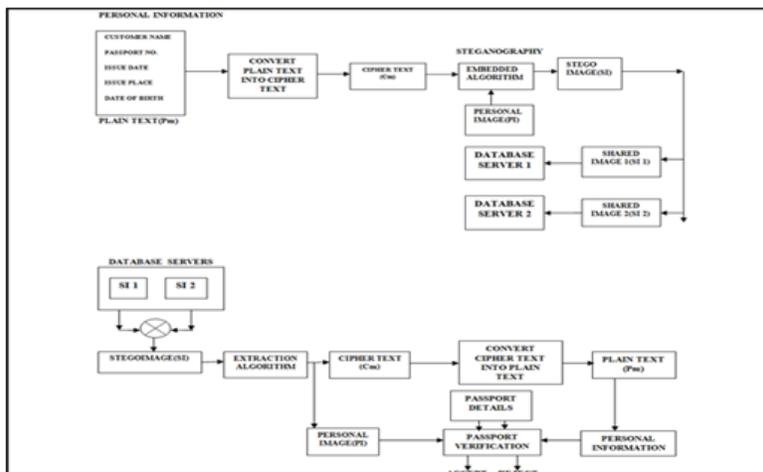


Fig.5. Proposed hybrid architecture for securing the data and image of an individual

CONCLUSION

Different techniques are followed by various researchers to achieve security to the template stored in the database servers. In this paper, the template is protected by using the techniques of steganography for the stored information and visual cryptography for the face images of corresponding individual. Thus the personal information along with the face image of an enrolled person is secured using this approach.

Scope for Future work

Simulate the hiding and retrieving algorithm using MATLAB tool or suitable software tool and obtain the performance analysis result. Use different images to obtain better PSNR value with high level of security. This paper only gives the idea to provide security to database server for passport verification system. This paper doesn't provide simulated result.

REFERENCES

- A.Vinodhini, M.Premanand, M.Natarajan, Visual Cryptography Using Two Factor Biometric System for Trust worthy Authentication, in International Journal of Scientific and Research Publications, 2(3), 2012, 1-5.
- Arun Ross and Asem Othman, Visual Cryptography for biometric privacy, in the IEEE transactions on information forensics and security, 6(70), 2011.
- Divya James and Mintu Philip, A Novel Face Template Protection Scheme based on Chaos and Visual Cryptography, in International Journal of Applied Information Systems, 2(5), 2012, 31-35.
- Divya.A and K.Ramalakshmi, Maintaining the Secrecy in Visual Cryptography Schemes in IEEE, 2011, 311-314.
- ForoughShami, Faranak Shamsafar and Hadi Seyedarabi, Securing Database of Biometric Systems, in 9th International ISC Conference on Information Security and Cryptology, 1-4, 2012.
- Nazanin Askari, Cecilia Moloney and Howard M Heys, Application of Visual Cryptography to biometric Authentication, 2011, 1-5.
- P.S.Revenkar, AnisaAnjum and W.Z. Gandhare, Secure Iris Authentication using Visual Cryptography, in International Journal of Computer Science and Information Security, 7(3), 2010, 217-221.
- Rachna, H M Rai, ChetanManchanda, Safeguarding Biometric Template Data: Risks And Protection Schemes, in International Journal of Applied Engineering Research, 7(11), 2012, 1-5.
- Rahna, P. Mohammed, A Secured Approach to Visual Cryptographic Biometric Template, in ACEEE International Journal on Network Security, 02(3), 2011, 15-17.
- Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo, Half-ton Visual Cryptography Via Direct Binary Search, in 14th European Signal Processing Conference (EUSIPCO 2006), 2006, 1-5.