isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337

Multilayer Security For Images Using Visual Cryptography And Steganography

K.N.Keerthana[1] S.Kavitha[2] R.Karthi[3] K.Lakksha[4]

Department of computer Science, Velalar college of engineering and technology

Anna university .Chennai, knkeerthana@gmail.com

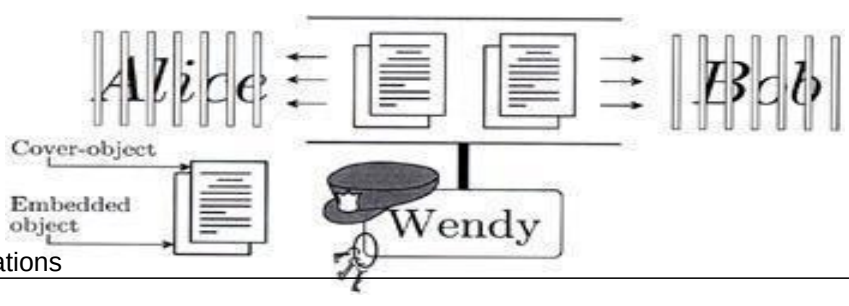
Abstract__*Recently, numerous novel algorithms have been proposed in the fields of steganography and visual cryptography with the goals of improving security, reliability, and efficiency. Privacy in communication is desired when confidential information is shared between two parties. Mainly this project uses DCT, IDCT, neural networks and visual cryptography. The proposed system provides multilayer security. The level of security is achieved by using steganography followed by visual cryptography. The secret image is embedded into the cover image. Then the encrypted image is divided into 3 shares. If the secret key valids, first share will be displayed. By analyzing the finger print and knuckle print, the embedded image obtained by combining the remaining shares and the extracted secret image will be displayed respectively. This project is implemented using Matlab software.*

Keywords: DCT, IDCT, neural networks, shares, Steganography, Visual Cryptography.

Introduction

Since the rise of internet one of the most important factors of technology is security of Images. Cryptography was created as a technique for securing secrecy of communication and many different methods have been developed to encrypt and decrypt the image. An important subdivision of Image Hiding is steganography. Sometimes it's not enough to keep contents of image secret but also it's necessary to keep existence of image secret. The technique used to implement this is called steganography. It's made up of 2 Greek words *stegos* meaning covered and *Grafia* meaning writing. Steganography is the art and science of invisible communication. The technique of steganography requires Cover Object(C), secret message (M), stego key and stego function (Fe) .

Fig. 1 Prisoners problem



STEGANOGRAPHY METHODS:

There are 3 ways namely

Injection - embeds secret message directly in host medium

Substitution – normal data is substituted with the secret data.

Generation of new files

STEGANOGRAPHY TECHNIQUES:

Steganographic techniques can be broadly classified as

1. Spatial domain techniques
2. Transform domain techniques
3. Hybrid domain techniques

In case of spatial domain technique all manipulations to the cover object and payload are done in time domain. LSB technique is the most popular spatial domain technique. Transform domain techniques are frequency domain techniques. Image is considered in terms of frequency components. DCT is the most commonly used technique. In case of hybrid domain technique image is divided into cells and then spatial or transform domain technique is applied. To illustrate the process of steganography we consider figure given below The classic model for invisible communication was proposed by Simmons as prisoner's problem. Alice and Bob are arrested are for some crime and they are thrown in different cells. They want to develop an escape plan but all communication is arbitrated by Wendy. She will not let them communicate through encryption and hence both parties should communicate invisibly – have to set up subliminal channel.

VISUAL CRYPTOGRAPHY:

It was proposed by Naor and Shamir in 1994. It's a scheme which encrypts image into shares but does not require any computations to get back the original image and it's an encryption technique used to hide images in such a way that decryption can be performed by human visual system if key is used. Here V.C operates on binary inputs and initially V.C was applied to black and white images but now it's extended to color and grey scale images. The easiest way to implement visual cryptography is to print two layers on transparencies.

HOW VISUAL CRYPTOGRAPHY WORKS?

Mainly visual cryptography operates on binary inputs. Hence natural images must be converted into halftone images using density of dots in order to simulate grey level. Binary data can be displayed

as transparent when printed on transparent screen. Each pixel of the image is divided into smaller blocks. There are always same numbers of black and white blocks. If a pixel is divided into 2 parts there is one black and one white block. If a pixel is divided into 4 parts there are 2 white and 2 black blocks.

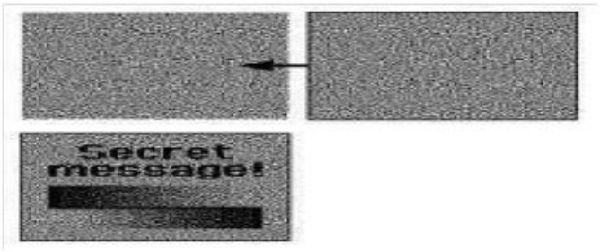


Fig- 2: example of visual cryptography

The basic model of visual cryptography proposed by Naor and Shamir accepts binary image I as secret image which is divided into n number of shares. Each pixel of image is represented by m sub pixels. The resulting structure of shared image is represented by S where S = [Sij], an n x m matrix. Any black and white visual cryptography scheme can be described using 2 n x m Boolean matrices (S0 and S1). S0 is used if pixel in the original image is white and S1 is used if pixel in original image is black. The important parameters in visual cryptography schemes are Pixel expansion (m) Contrast (β) The formula to compute contrast in different visual cryptography schemes is B = αm. In V.C white pixel is represented by 0 and black pixel is represented by 1. There are different visual cryptography schemes such 2 out of 2, 2 out of n, n out of n and k out of n V.C Scheme. The most commonly used is 2 out of 2 schemes. The relative difference α and contrast β is ½ and 1.

Fig - 3: construction of (2, 2) VCS

There are 2 collections of matrices C0 and C1. To share a white pixel we choose one of the matrix in C0 and to share black pixel we choose one of the matrix in C1. The first row of chosen matrix is used for share S1 and the second row is used for share S2. The disadvantage is that for every pixel encoded from original image into 2 sub pixels and placed on each share – shares have size of s x 2s

if secret image is of size s x s. There is a distortion hence we go for 4 sub pixel layout design. Here pixel is expanded into 2 x 2 sub pixels. The relative difference α and β is ½ and 2 respectively.

RELATED WORKS:

FINGER KNUCKLE ANATOMY:

Each finger has three joints .There are three bones in each finger called the proximal phalanx, the middle phalanx and the distal phalanx.The first joint is where the finger joins the hand called the proximal phalanx. The second joint is the proximal interphalangeal joint, or PIP joint. The last joint of the finger is called the distal interphalangeal joint, or DIP.

Fig. 5 Finger Knuckle Anatomy

Choosing the biometrics is the challenging task for researcher. Biometrics based authentication is just impossible to help us if we don't know what are the requirements.Biometrics authentication must provide the security level, unattendedsystem, Spoofing and Reliability. [21] Among all the modalities FKP broadly explored which has not yet attracted significant attention of researchers. Finger knuckle is user-centric, contactless and unrestricted access control. As it is contactless hence no chance of proof of physical presence i.e. antispoofing. Finger knuckle has High textured region. Many samples are available per hand and independent to any behavioral aspect. No stigma of potential criminal investigation associated with this approach. Table I shows the comparison between the biometrics traits.

Table I: Comparison of Biometrics Traits

Biometric Technology	Accuracy	Cost	Devices	Social acceptability	Interference
FKP	High	High	contactless	High	
Iris recognition	High	High	Camera	Medium low	glasses
Retinal scan	High	High	Camera	Low	irritation
Facial recognition	Medium low	Medium	Camera	High	Accident etc
Voice recognition	Medium	Medium	Microphone Telephone	High	Noise ,cold
Hand geometry	Medium low	Low	Scanner	High	Arthiritis ,rheumatism
fingerprint	High	Medium	Scanner	High	Dirtiness,injury, roughness
Signature recognition	Low	Medium	Optic pen Touch panel	High	Changeable or easy signature

Many Finger knuckle authentication algorithms for feature extraction have been implemented with different techniques.

Features of FKP Sensor

Parameter	Size (LxWxH)	Captured Image Size	Resolution	Distance between camera and finger knuckle	Background	Remark
FKP1	213mmX 413mm X271mm	640X180	NM	NM	Black	Large database of Hand
FKP2	NM	1600X1200	NM	20cm	White	little finger gave poor result
FKP3	160mmX125 mmX 100mm	768X576	140dpi	NM	NM	Computational time is high
FKP4	NM	640X480	13Mega pixel	NM	Black	Less number of users
FKP5	140mmX120 mmX 130mm	4300X3200	14Mega pixel	10cm	White	----

FINGERPRINT BIOMETRIC CONCEPT:

FP biometric is the commonly used oldest and solely method internationally accepted as legal method to identify a person. FP is the impressions of the minute ridge (called as dermal) of the finger. FP ridges and valleys are unique and unalterable. FP biometric is used in numerous applications that include civilian and commercial applications like military, law enforcement, medicine, education, civil service, forensics, driver license registration, cellular phone access [2], [3], computer log-in and like [4]. Today live FP readers based on optical, thermal, silicon, ultrasonic approach are used instead of old method of ink to capture FP. FP identification is based on minutiae or location and direction of the ridge endings and bifurcations (splits) along a ridge path. The two commonly used FP matching techniques are minutiae-based matching and pattern matching. Pattern matching just compares two image for checking similarity. Minutiae matching relies on minutiae points i.e. location and direction of each point. Experimental results show that the fingerprint based systems have very low FRR (False Rejection Rate) of 3 to 7% and 0.001 to

0.01% of FAR (False Acceptance Rate). The pre-requisite to match the FP is classification. The classification is treated as course level matching. The FP can be classified as whorl, right loop, arch, tented arch. In order to ensure the performance of FP identification, enhancement algorithms are needed to improve clarity of input fingerprint images.

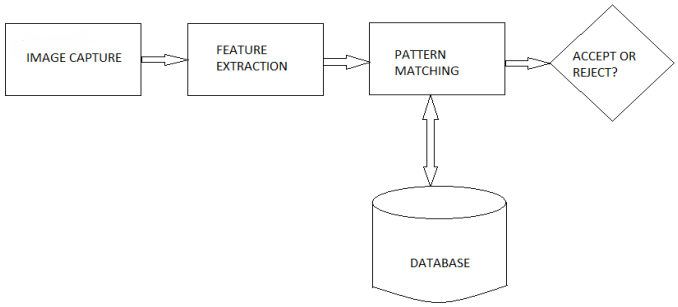
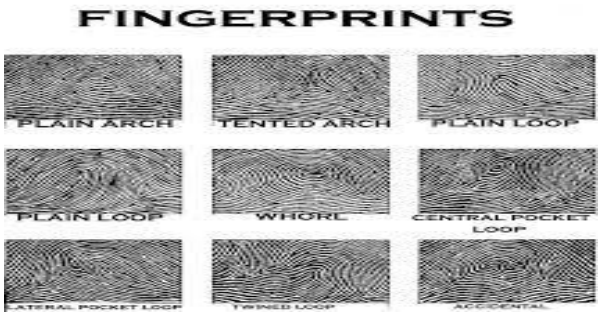


Fig. 6. Biometric system.

The customary FP pattern types are:



PROPOSED METHODOLOGY:

THE BASICS OF EMBEDDING:

Three basic aspects in information-hiding systems are: **security**, **capacity**, and **robustness**. Security refers to an inability of eavesdropper to detect hidden information. Capacity is the amount of information that can be hidden in the cover medium. And Robustness is the amount of modification to the stego medium can bear before an adversary can destroy hidden information. Information hiding can be relates to both watermarking and steganography. Following Figure shows a simple representation of the general embedding and decoding process of steganography. In this a secret image embedded inside a cover image which produces the Stego Image.

Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337

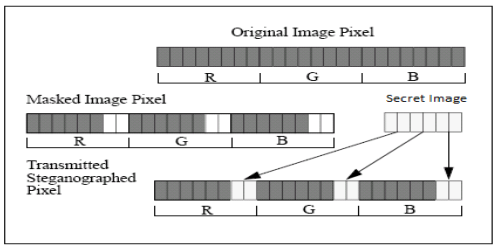
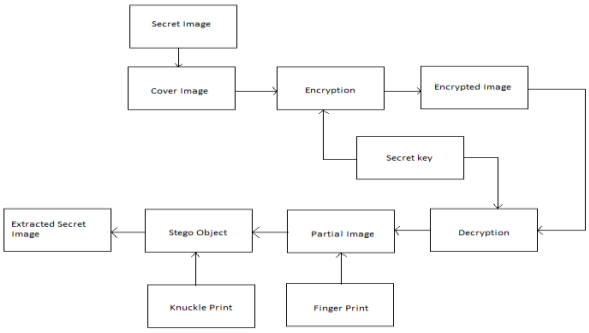


Figure 4 : Embedding Data in RGB Pixel

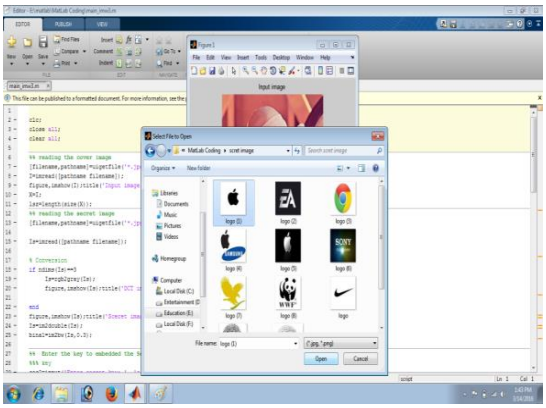
PROCESS OF ENCRYPTION AND DECRYPTION DATA :

In the encryption, one or more protocols will be used to embed the secret image into the cover image. The type of protocol will depend on image you are trying to embed and what you are embedding it in. A key is also needed in the embedding process. Embedding the image in this way, you can reduce the chance of a third party [1]. In general the embedding process inserts a sign, S, in an object, O. A key, K, mostly produced by a random number generator is used in the embedding process and the resulting signed object, O' is generated by the mapping: O x K x S → O'. After embedding, encryption is done and the encrypted image is divided into 3 shares, then it will be sent via some communications channel, like Email, to the intended recipient for decrypting. The recipient must decrypt the encrypted image in order so he can view the secret image. The decrypting process is just the reverse of the encrypting process. In the decrypting process, the encrypted image is fed into the system.The key,used for the encryption is needed to get the first share of the encrypted image.Then the finger print is needed to obtain the stego image by combining the remaining shares.Stego image is the original cover image which contains the secret image embedded in it. This image should look almost identical to the cover image otherwise a third party attacker can detect the embedded image. From the stego image,we extract the secret image by using knuckle print. The general decryption process again requires a key, K, this time along with a signed object, O'. Also required is either the sign, S, or the original object, O, and the result will be either the retrieved sign, S from the object or indication of the likelihood of S being present in O'. Image Steganography has attracted extensive research as well as popular usability in recent years. This is due to the fact that huge amounts of data can be hidden without perceptible impact to the carriers because of the popularity of electronic images that are widely available.so we describe steganography techniques and tools that uses image files in more details [4].

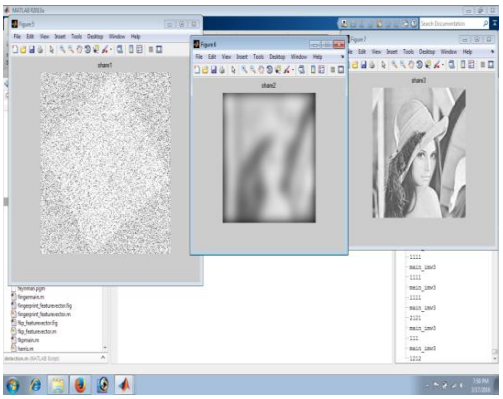


EXPERIMENTAL RESULT:

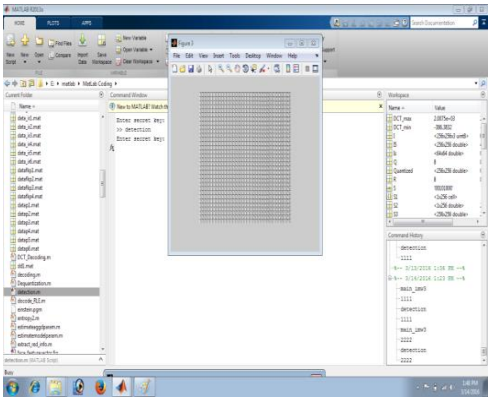
SELECTING COVER IMAGE AND SECRET IMAGE:



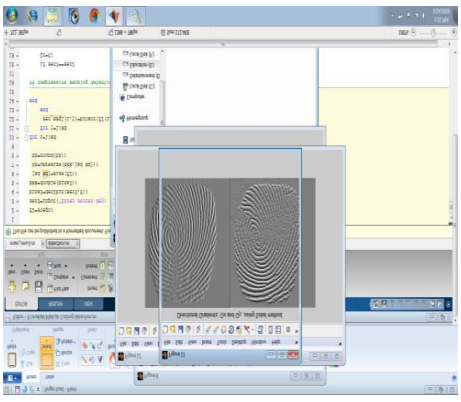
SHARES OF ENCRYPTED IMAGE:



SECRET KEY VERIFICATION:



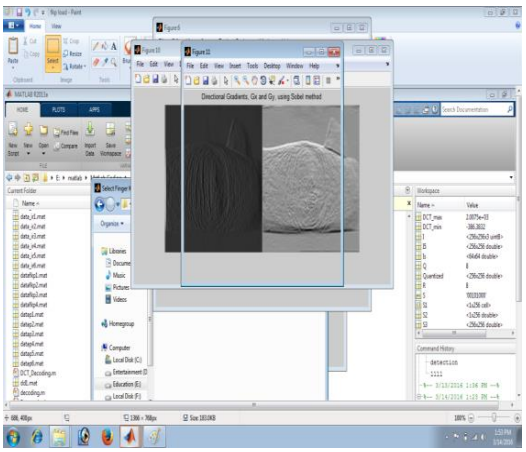
FINGER PRINT ANALYSIS:

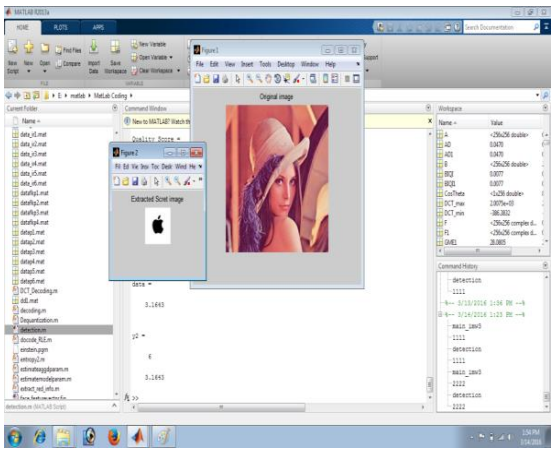


KNUCKLE PRINT ANALYSIS:

EXTRACTED SECRET IMAGE:

Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337





CONCLUSION

This project implemented the steganography, visual cryptography and the combination of both. This project allows the authorized users to work. The algorithm developed can be used depending on the situation and application. The proposed system is aimed to simplify the complex and redundant process with the flexibility of a simple process. The proposed system is being developed as an attempt to overcome the difficulties of the existing system. The following are the merits of the proposed system. It provides multi levels of security to the image being transmitted. That is the intruders cannot easily break the system. Even if they realize the existence of a secret image they cannot easily recognize the image, since image is hidden. This system overcomes the demerits of using single level of hiding. That is either using cryptography or steganography. And one more thing to add is it requires only the computation time of single level hiding, because visual cryptography requires no computation to decrypt the information.

APPLICATIONS:

In military and navy to make their communication secure In payment gate way.

In medical production system for secret products

In business dealing and settlement contracts

In electronic mail communication

.

REFERENCES

[1] Mahmoud Hanan,Al-Dawood Aljoharah [2010] Novel Technique for Steganography in fingerprints Image : Design and Implementation Sixth International conference on Information Assurance and Security .

[2] Marvel L.M [1999] Spread Spectrum Image Steganography, IEEE TRANSACTION ON IMAGE PROCESSING,vol. 8 ,Pp- 1075-1083

[3] L. Hong, Y. Wan, A. Jain, Fingerprint image enhancement: algorithm and performance evaluation , IEEE Transactions on Pattern Analysis and Machine Intelligence 20 (8) (1998) 777 789.

[4] Q. Zhao, D. Zhang, L. Zhang, N. Luo, Adaptive fingerprint pore modeling and extraction, Pattern Recognition 43 (8) (2010) 2833–2844.

[5] C. Han, H. Cheng, C. Lin, K. Fan, Personal authentication using palm-print features, Pattern Recognition 36 (2) (2003) 371–381.

[6] D. Zhang, W. Zuo, F. Yue, A comparative study of palm print recognition algorithms, ACM Computing Surveys 44 (1) (2012) 2:1–37.

[7] S. Mil'shtein, A. Pillai, A. Shendye, C. Liessner, and M. Baier, ―Finger print recognition algorithms for partial and full fingerprints,‖ in *Proc. Technologies for Homeland Security*, IEEE, 2008, pp. 449-452.

[8] Y. N. Shin, Y. J. Lee, W. Shin, and J. Choi, ―Designing fingerprint-recognition-based access control for electronic medical records systems,‖ in *Proc. 22nd International Conference on Advanced Information Networking and Applications – Workshops*, IEEE, 2008, pp. 106-110.

[9] Y. Wang, L. X. Yao, and F. Q. Zhou, ―A real time fingerprint recognition system based on novel fingerprint matching strategy,‖ in *Proc. the Eighth International Conference on Electronic Measurement and Instruments*, 2007, pp. 1-81-1-85

[10]. Websites like Google, Wikipedia.