IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Enhancing the security of Biometric Authentication Based on Visual Cryptography and Watermarking Technique

***1 Mrs. Manju M., *2 Ms. Anita Madona M.,**

*1 M.Phil Research Scholar, Department of Computer Science Auxilium College (Autonomous), Vellore, TamilNadu, India

*2. Assistant Professor, Department of Computer Science Auxilium College (Autonomous), Vellore, TamilNadu, India.

Abstract: -A new plan for user authentication is proposed using visual cryptography and invisible digital watermarking. Visual cryptography allows visual information to be encoded in such how that decoded becomes the work of the person to decrypt via a sight reading. Security for identity-based identification using visual cryptography and watermarking provides secure authentication for user access. To ensure a protective authentication in visual cryptography and watermarking algorithm embedding of finger print, iris image and face recognition are often used. A user verification and authentication methods are not suitable for frequent verification. The traditional behavioral biometrics on PCs, such as keystroke and mouse dynamics, cannot be practical on for user verification. Existing reauthentication schemes for fingerprint, iris image and face recognition are not practical for real applications due to low accuracy. To overcome such issue, we can utilize the support vector machine which provides the high accuracy, which involves two design methodologies, first is False Acceptance Rate (FAR) and second is False Rejection Rate (FRR). To enhancing the security of existing technique like finger print, iris image and face recognition over Noisy Images, an efficient image segmentation technique such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) is used. To possess accurate FAR Extraction Ratio of Co-efficient (ROC) Curves, the result of MASEK and Ma are obtained. Binomial Distribution vector space is executed for FAR and FRR. To know Distribution Reliability in Ma and MASEK in 128 bit blocks are applied. The 128 bit block used for image segmentation uses DCT, DWT and DFT technique. The uniqueness of the input image totally results in distortion problems, so a robust watermarking algorithm and visual cryptography is used to develop the security, which can prevent the image from being hacked as well as distorted. The Mat Lab framework for Experimental results indicates that the proposed watermarking algorithm has high security, watermarking life time, user authentication delay and perceptual invisibility. Moreover, it can detect and locate the tampered region effectively for various performances of finger print, iris and Face. The Experimental result shows that Min & Max of FAR and FRR rate for security management control for visual cryptography.

Key Words: *Data Encryption Standard (DES), Advanced Encryption Standard (AES), Visual Cryptography, Watermarking*

I. INTRODUCTION

Visual cryptography is presented to preserve the security of biometric information (viz., raw images) by deteriorating the new image into two images in such a manner when both images are at the same time accessible in the original image can be exposed; more the discrete component images do not expose any information almost the original image. During the verification process, the reliable individual sends a demand to each Biometric and the equivalent sheets are transmitted to it. Sheets are overlapped (i.e. superimposed) in order to recreate the security image thereby avoiding any complex decryption and decoding computations that are used in watermarking or cryptosystem approaches. When the matching score is executed, the reconstructed image is discarded.

Watermarking focuses on the works the watermarking methods that do not directly embed watermarks into the original digital images. Instead, verification information is generated which is used to verify DCT, DFT and DWT. It generates the technical feature of coefficient pixel on the watermarking technical. It reduces the mean square error of FAR and FRR.

The term biometrics allows a person to be distinguished and confirmed dependent on conspicuous and irrefutable information, which are remarkable and definite to them. Biometrics is the most reasonable method of recognizing and confirming people in a dependable and quick manner through exceptional organic attributes. There are various physiological just as social biometric attributes like fingerprints, iris, face, hand calculation, voice, step, and so on, at risk on kinds of utilizations.

Biometric traits are increased by implementing extracted devices and unique features to create a biometric pattern in the acceptance process. There are various applications are involved in personal identification is required such as time and attendance, passport, controls, airport, mobile phones, health and social services, computer login control, secure electronic banking, bank ATM, credit cards, etc. There are various issues are correlated to biometric method and biometric data. Biometric systems are susceptible to attacks, it can decrease their security. The taken patterns can furthermore be used for other unintended purposes, e.g. accessing unauthorized user smart card transactions or accessing fitness interrelated records. Therefore, biometric patterns should not be stored in plaintext form to protect the biometric data and template visual cryptography and watermarking can be used. This thesis proposes a system using visual cryptography and watermarking method to protect the finger print, iris template and face recognition in order to create user authentication secure from unauthorized access in system database.

II. Related work

Visual cryptography is a cryptographic method which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image. Visual Cryptography is an encryption procedure dependent on the secret sharing problem. In this situation, visual information is shared, i.e., the message to be encoded can be a black and white image, grey scale or a colored one, printed text, etc. The encryption of the secret is done in such a way, that its decryption is very simple since there is no need for any numerical calculations; it is done automatically by the human eye. Biometrics is body estimations and calculations related to human features. Biometrics validation (or accurate confirmation) is used in computer science as a form of recognizable proof and access control. It is additionally used to identify individuals in crowds that are under observation. Biometric identifiers are the particular, quantifiable qualities used to name and depict people. Biometric identifiers are regularly arranged as physiological and social qualities. Physiological qualities are identified with the state of the body. Models incorporate, fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including typing rhythm, gait, and voice. More customary methods for access control incorporate token-based recognizable proof frameworks, for example, a driver's permit or visa, and information-based ID frameworks, for example, a secret key or individual ID number. Since biometric identifiers are interesting to people, they are more dependable in checking character than token and information-based techniques; in several case, the assortment of biometric identifiers raises protection worries about a definitive utilization of this data. Further specially, the attacker expresses the encryption change as a lot of multivariate polynomial equations and tries to improve the encryption key by resolving the system. In contrast, algebraic attacks exploit the intrinsic algebraic structure of a cipher. More specifically, the attacker expresses the encryption transformation as a (large) set of multivariate polynomial equations, and subsequently attempts to solve such a system to recover the encryption key.

Fingerprint

Every individual has a unique fingerprint which consists of edges, grooves, and direction of the lines. The fingerprints contain of three types: arch, loop, and whorl. The fingerprint uniqueness is decided by these features also as minutiae features like bifurcation and spots (ridge endings). The impression of fingerprint verification is that the method and compare a fingerprint and to match both the fingerprints. This process is especially used to verify a person’s authenticity. For verification an individual must his or her fingerprint into the fingerprint verification system. Then its representation is saved in some compressed to the read format with the person’s identity and his or her name. Then it's applied to the fingerprint verification system in order that the individual identity is often easily verified. Fingerprint verification is additionally called as one-to-one matching. Fingerprint identification is especially wont to specify any person’s identity by his for fingerprint. Identification has been used for criminal fingerprint matching. Here the system matches the fingerprint of unknown person against the opposite fingerprints present within the database to associate a criminal offense with identity. This process is additionally called together too many matchings. Identification is conventionally used to solve crime.

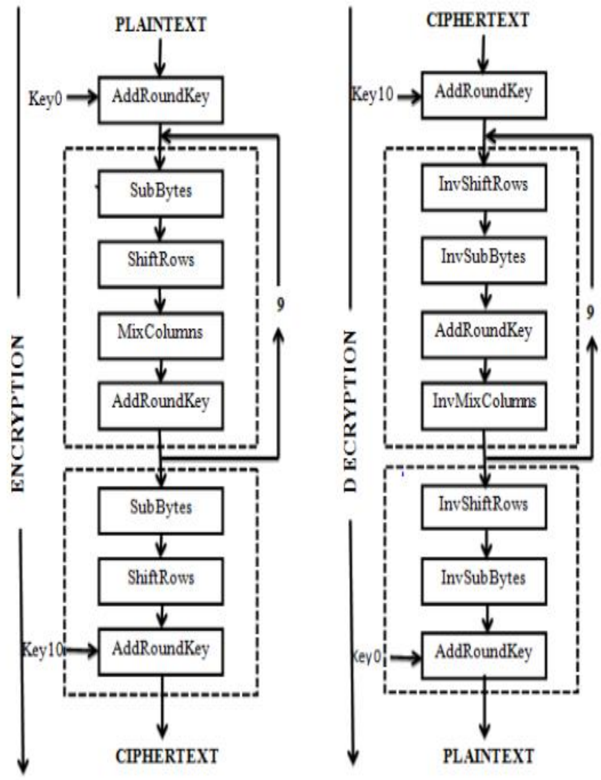


Fig 1: Structure

III. PREVIOUS IMPLEMENTATIONS

Visual Cryptography (VC) to encode a secret employing a (2, 2) VC Scheme, the unique image is separated into two shares such that every pixel in the original image is swapped with a non-overlapping block of two sub-pixels. Somebody who holds only one share will not be able to uncover any data about the secret. To decrypt the image, every one of these shares is equally onto a transparency. Stacking both these transparencies will allow visual recovery of the secret. Biometric Image (Fingerprint, Iris and Face) represents the plan of encoding one pixel in a (2, 2) VC scheme. A white pixel is split into two equal blocks of sub-pixels. A black pixel is split into two complementary blocks of sub-pixels. While creating the shares, if the given pixel *p* in the original image is white, then the encoder randomly selects one of the first two columns of biometric image (Fingerprint, Iris and Face). If the given pixel *p* is black, then the encoder randomly selects one of the last two columns of Biometric image. Each block has half white and half black sub-pixels, independent of whether the consistent pixel in the secret image is black or white. All the pixels in the remarkable image are encrypted correspondingly using independent random selection of columns.

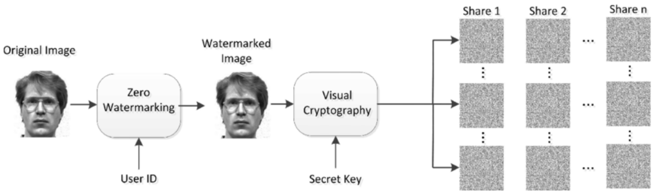


Fig 2: visual cryptography with watermarking

Visual encryption was designed to encrypt and decrypt secret images without using complex cryptographic calculations. This has prompted to the enhancement of visual cryptography for associated fields such as secret sharing, biometrics and watermarking. For the future work, expected for the security of watermarked biometric images, the encoding and decoding procedures are using Fingerprint, iris and face images.

A watermarking system is typically divided into three different phases: inserting, attack and detection. In the inserting phase, a binary matrix is generated from the host image and a secret key. This binary matrix, along with the secret binary image (watermark), produces a Master Share allowing to the predefined encryption rules of the Visual cryptography Scheme. The Master Share has to be enrolled with a confided in outsider for additional verification. The watermarked biometric verification image is normally transmitted or stored. In that event that an individual makes an alteration to the marked image, it is called an attack. While deciding the rightful ownership, the same secret key is used to produce the Verification Share. Then the Verification Share and the Master Share (kept by the trusted third party) are joined to recover the hidden watermark.

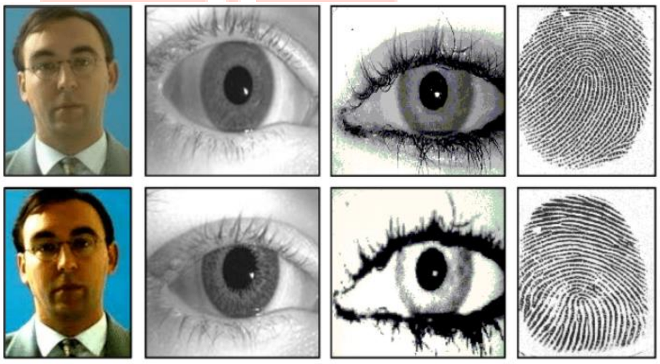


Fig 3: Example of images captured from real face, iris and fingerprint (upper row) and from watermarking (lower row): (From left to right) face photo attack, iris printed contact lens watermarking, iris photo attack, fingerprint latex Visual cryptography

Analysis liveness detection methods examine the skin properties, such as skin surface and skin reflectance, under the presumption that surface properties of genuine faces and prints, e.g. shades, are different. Examples of detectable surface patterns due to artifacts are printing failures or blurring a method for print-attack face DCT with DFT by exploiting differences in the 2-D Fourier spectra of live and spoof images. The method only works fine for down tested pictures of the attacked identity, but likely fails for higher-quality samples. Considered Lambertian reflectance model with difference-of-Gaussians (DoG) to derive differences of motion deformation patterns between 2-D face photos presented during DCT with DFT using visual cryptography and 3-D live faces. Exploited the Retinex reflectance models to differentiate spoofed and live faces. Watermarking developed micro-texture analysis based methods to detect printed photo-using visual cryptography. One limitation of presented methods is the requirement of reasonably sharp input image. Other countermeasures against face DCT with DFT using visual cryptography include multispectral imaging, which analyze the reflectance of object surfaces and thus discriminate live faces from fake ones

IV. SYSTEM IMPLEMETNATION

Fingerprint, Iris and Face of an image is a method by which the information related to the image and its owner can be kept hidden in the image (cover image) itself. A unique image identification number, customer id and name of the image will be used as the fingerprint, Iris and Face of each image buy-sell transaction. This unique finger print, Iris and Face will be embedded into that particular image. The fingerprint, Iris and Face will be generated using a text to image conversion algorithm by which secret data will be prepared. The novelty of the algorithm lies in the fingerprint, Iris and Face method. It is visually encrypted to enhance the security. The fingerprint, Iris and Face is divided into some shares of equal size which alone does not contain any significant information about the fingerprint, Iris and Face unless they are visually overlapped one above the other. The complete information in the finger print, Iris and Face is divided equally among all the shares.

It is visually watermarking to enhance the security. The fingerprint, Iris and Face is divided into some shares of equal size which alone does not contain any significant information about the finger print, Iris and Face unless they are visually overlapped one above the other. The complete information in the fingerprint, Iris and Face is divided equally among all the shares. To serve the fingerprint, Iris and Face purpose the shares are embedded into the image in different blocks in the frequency domain. A single cover image will contain all the shares of the finger print, Iris and Face. So whole information about the finger print, Iris and Face is inside the cover image but embedded into different spatial locations. This involves a new strategy of embedding multiple watermarks in the same image. Each share can be seen as an independent watermark and will be embedded into a different block of the image.

The method proposed here is supposed to be very robust. The fingerprint, Iris and Face is secure against the general image processing using visual cryptography like noise addition and image compression. The main benefit of using a visually encrypted fingerprint, Iris and Face is that there is no effect of the normal correlation of the fingerprint, Iris and Face to the image. Blind detection of the fingerprint, Iris and Face to illegally detect it is not possible since the correlated fingerprint, Iris and Face will appear as noise only. Even some shares of the fingerprint, Iris and Face get detected but without the successful detection of every share it is impossible to regenerate the fingerprint, Iris and Face. So, no illegal person can detect the finger print, Iris and Face without knowing the all the shares altogether.

Generation of fingerprint, Iris and Face: The logos of organizations or some standard images have been used by the watermarking fraternity worldwide. But these are not image and customer dependent, which is the basic need for a fingerprint, Iris and Face. So, what we propose here to generate a unique finger print, Iris and Face for every image. This fingerprint, Iris and Face will contain in information about the customer and the image itself in the form of text. This text will be converted into image which will finally be used as a fingerprint, Iris and Face.

4.1 Finger Print Analysis

Fingerprint analysis is quite an ancient practice. A fingerprint acknowledgment system can be misled by (i) a 2-D (flat) fake fingerprint of a real user; (ii) a 3-D fake fingerprint of a real user. Fake fingerprint can be fabricated either by 'consensual/cooperative/direct casts' or 'non-consensual/ non cooperative/indirect casts' method uses easily available materials like latex etc. In consensual method, the fake fingerprints are generated directly from real fingers with individual's consent, while in non-consensual technique fake fingerprints are fabricated from latent finger marks on everyday use items or sensors; hence, the participation of the user is not needed. Software based fingerprint liveness detection can be grouped in 5 groups: perspiration-based, skin deformation-based, image quality based, pore detection-based, and combined approaches.

4.2 Embedding Procedure

This scheme assumes that the binary secret image (watermark) S of size wxh is to be embedded into the host image H of size rxc. Let K be a random integer choosed by the user as a secret key. The output of the inserting phase is a watermarked image O of size rxc (same as the original host image) and a Master Share M of size wx2h.

Inputs: A Host Image H, a Binary Watermark S, and a Secret Key K

Outputs: Marked Image O and a Master Share M

The watermark embedding procedure is as follows:

Step1: The secret key *K* is used as a seed to generate *wxh* random numbers over the interval [*1 to rxc*]. Let R_i be the i^{th} random number.

Step2: Creation of a binary matrix *X* of size *wxh* such that the entries in the array are the most significant bits of R_i^{th} ^{pixel} of the host image.

Step3: Creation of a binary matrix *Z* of size *wxh* such that the entries in the array are the most significant bits of the R_i^{th} random number.

Step4: Creation of a binary matrix *Y* of size *wxh* such that $Y_i = XOR\ (X_i, Z_i)$

Step5: Creation of a Master Share M by assigning a pair of bits for each element in the binary matrix Y according to the predefined encryption rules of VC as shown in Table 2. Finally, the Master Share is registered with a trusted third party.

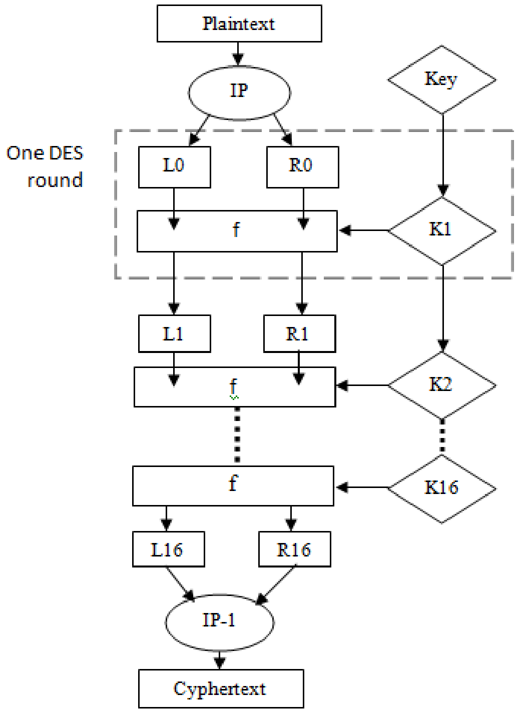


Fig 4: Embedding Algorithm

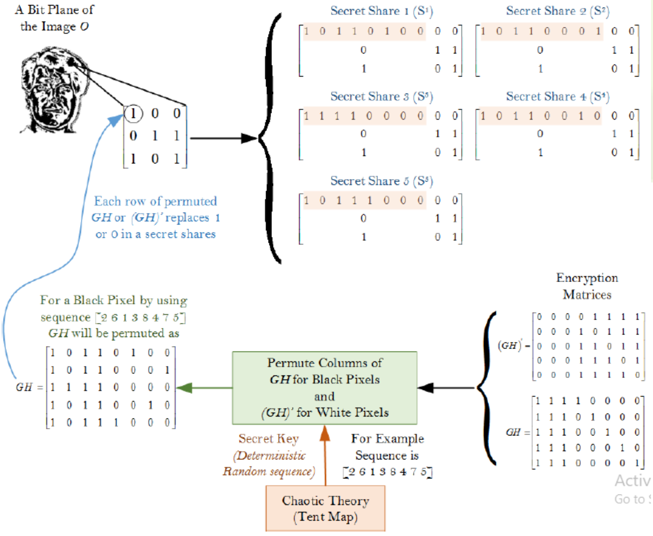

A Bit Plane of the Image O
Secret Share 1 (S¹)
Secret Share 2 (S²)
Secret Share 3 (S³)
Secret Share 4 (S⁴)
Secret Share 5 (S⁵)
Each row of permuted GH or (GH)' replaces 1 or 0 in a secret shares
For a Black Pixel by using sequence [2 6 1 3 8 4 7 5] GH will be permuted as
GH =
Permute Columns of GH for Black Pixels and (GH)' for White Pixels
Encryption Matrices
(GH)' =
GH =
Secret Key (Deterministic Random sequence)
For Example Sequence is [2 6 1 3 8 4 7 5]
Chaotic Theory (Tent Map)

Fig 5: System Analysis using Finger print, Iris and Face

Algorithm Implementation

Step 1: First divide the 128-bit block into eight 4-bit words

Step 2: Attach an additional bit on the left to each 4-bit word that is the last bit of the previous 4-bit word

Step 3: Attach an additional bit to the right of each 4-bit word that is the beginning bit of the next 4-bit word.

Step 4: The 1024-bit key is divided into two halves, each half shifted separately, and the combined 1024-bit key permuted/contracted to yield a 128-bit round key.

Step 5: The 48 bits of the expanded output produced by the are XOR ed with the round key. This is denoted to as key mixing.

Step 6: The output generated by the previous step is broken into eight six-bit words. Each six-bit word goes through a substitution step; its replacement is a 4-bit word. This substitution is carried out with the S-box. The aim of the substitution is executed by the S-box to present diffusion in the generation of the output from the input. Diffusion means that each plaintext bit must affect as many cipher text bits as possible. The approach used for making the different round keys from the core key is meant to present confusion into the encryption process.

Color of i^{th} pixel in binary watermark (S_i)	i^{th} entry in binary array (Y_i)	Pair of bits to be assigned in master share
Black	1	(0, 1)
Black	0	(1, 0)
White	1	(1, 0)
White	0	(0, 1)

Confusion in this framework means that the association between the encryption key and the cipher text must be as difficult as possible. Another way of describing confusion would be that each bit of the key must affect as many bits as possible of the output cipher text block.

Mix Column

This is perhaps the hardest step to both understand and explain. There are two parts to this step. The first will explain which parts of the state are multiplied against which parts of the matrix. The second will describe how this multiplication is applied over the Galois Field

$W(I) = W(I - 8)$ XORW $(I-1) I$ is not a multiple of 16
$W(I) = W(I - 8)$XOR $T(W(I-1))$ I is a multiple of 16

Where the T (I) transformation is defined as:

T(I)=Byte Sub(Shift Left(W(I)))XOR Round Const

The round constant is defined by the following equation:

Round Const = $00000010^{(i-16)}/^{16}$.

Key Expansion and Rounds

The 1024-bit input key of the new AES-1024 algorithm is used to generate ten sub-keys for each of the ten AES rounds. The round ±keys expansion process involves arranging the original 512-bits input key into eight words of eight bytes each.

Key Expansion (byte key[4 * Nk], word w[Nb * (Nr + 1)], Nk)
Begin

```
    i = 0
    while (i < Nk)
    w[i] = word [ key[4*i], key[4*i+1], key[4*i+2],
            key[4*i+3] ]
    i = i + 1
    end
    i = Nk
    while (i < Nb * (Nr + 1))
      word temp = w[i- 1]
      if (i mod Nk = 0)
        temp = SubWord(RotWord (temp)) xor Rcon[i/Nk]
      else if ((Nk = 8) and (i mod Nk = 4))
         temp = SubWord(temp)end ifw[i] = w[i - Nk]
                 xor tempi = i + 1
     end while
End
```

Detection Procedure

Detection (also called extraction) is an algorithm which is applied to the attacked image to extract the watermark from it. In robust (secure) watermarking applications, the extraction algorithm should be able to reproduce the watermark, even if the modifications were strong.

Inputs: Modified image O', Master Share M, and a Secret Key K

Output: Extracted Watermark S'

The watermark detection procedure is as follows:

Step1: The secret key K is used as a seed to generate wxh random numbers over the interval [1 to rxc]. Let R_i be the i^{th}random number.

Step2: Creation of a binary matrix X of size wxh such that the entries in the array are the most significant bits of $R_i^{th\ pixel}$ of the host image.

Step3: Creation of a binary matrix Z of size wxh such that the entries in the array are the most significant bits of the R_i^{th} random number.

Step4: Creation of a binary matrix Y of size wxh such that Yi= XOR (Xi, Zi)

Step5: Creation of a Verification Share such that, if the element in the binary matrix Y is '0' then Vi= (0, 1) has to be assigned, else Vi= (1, 0) has to be assigned.

Step6: The secret image can be extracted by performing logical OR operation as follows: Si' = OR (Mi, Vi).

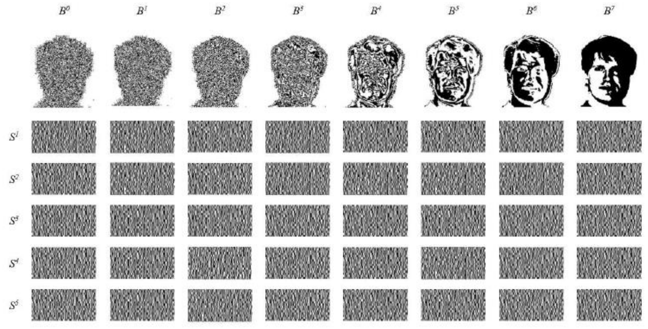


Fig 6: Secret shares for all bit planes B0, B1, B2, B3, B4, B5, B6, and B7.

4.3.1 Cryptography with fingerprint, Iris and Face

Input: An m × n cover image and authenticating message/image.

Output: Two shares, each of size m × 2n.

Step1: Generate Watermarked Image by Using Visual Cryptographic decryption

1. Start
2. Take a input bio authentication image and Cover Image
3. Subdivision of Image into three level bio authentication, Fingerprint, IRIS and Face
4. Generated the Bio authentication process using authentication process only
5. Apply DCT,DWT and DFT method using mid-band coefficient

Step 2: Retrieval of Fingerprint, Iris and Face

1. Start
2. We take output data in form of image data for example consumer id, unique image no., image name etc.
3. This secure information is extraction into cover image
4. Then we get watermarked secure image and Data Analysis for pixel value to get bio metric information capture the image and shared images.

4.3.2 Receiving side Decoding Algorithm

Input: Two shares, each of size m × 2n.

Output: The original cover image and an authenticating message/image.

Step 1: Do till the end of the share matrices.

Step 2: Take two consecutive pixel values from each of the share.

Step 3: Evaluate whether these represents one black pixel or white pixel using the above mentioned concept.

Step 4: If it is a white pixel then discard the 0 values and calculate the original pixel value from other pixel values by the equation 4 and equation 5.

Step 5: Else discard the 255 values and calculate the original pixel value from other pixel values by the equation 6.

Step 6: Repeat for each group of four pixel values of the reconstructed authenticated image.

Step 7: Calculate 8-bit representation of each of 4 consecutive pixels of authenticated image and put it into an array N1 (0-7), N2 (0-7), N3 (0-7), N4 (0-7).

Step 8: count <-0; i<-1;

Step 9: While (count 6) {

Step 10: Find the extraction positions P and P+1 for L(count) and L(count+1) respectively using equation 1 where L(0-7) representing each character/pixel of authenticating message/image.

Step 11: Replace L (count) by Ni (P) and L (count+1) by Ni (P+1);
Step 12: If (243 decimal value of Ni (0-7) 255) then store the value 255 in data storage 1.
Step 13: Else if (0 decimal value of Ni (0-7) 12) then store the value 0 in data storage
Step 14: i=i +1 and count= count+2;}
Step 15: Store the corresponding character/pixel value of L (0-7) in data storage 2.
Step 16: Stop.

EVALUATION RESULT:

At the point when plants are tainted by pathogens, they make spots of various shapes. Shapes can change according to the kind of pathogen, sort of finger, face and iris species, and kind of maladies. Sporadic, curved, oval, rectangular, round shapes are made by pathogens. In image preparing strategies, territorial properties have been utilized to depict and speak to the shapes. The fragmented image is changed over into a double image and the quantity of associated parts is computed. Territory and centroid of each associated segment are ascertained. The territory is the quantity of white pixels in a given image and centroid is the focal point of mass of the given locale. To diminish the time required for the extricating state of every segment, the part having most extreme region is edited.

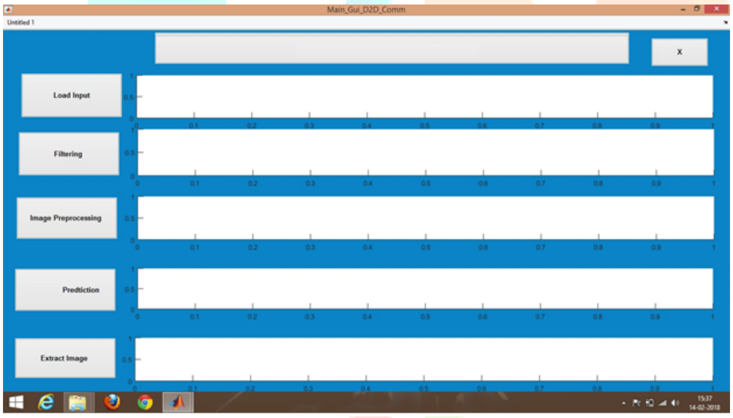


Fig 7: Data Analysis for raw side view fingerprint, iris and face recognition

Change over the standardized RGB image into FAR space. FAR shading space has been utilized principally for division of finger, face and iris ailments in view of underneath reasons 1) In FAR plane contaminated part can be effectively distinguished 2) The shading contrast of human segregation can be specifically articulated by Euclidean separation in the FAR shading space 3) The force and chromatic segments can be utilized independently and 4) Plant tainted spots frame little groups in Cr space

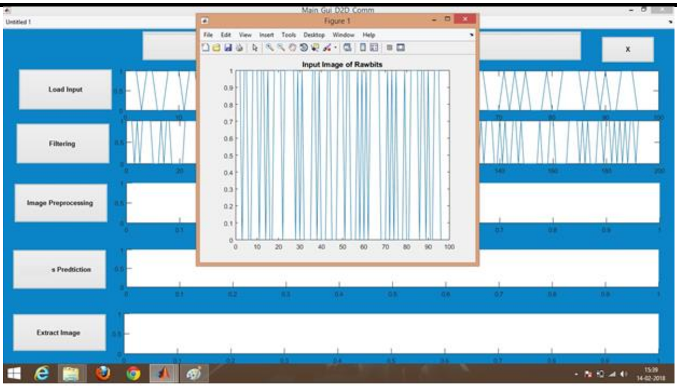
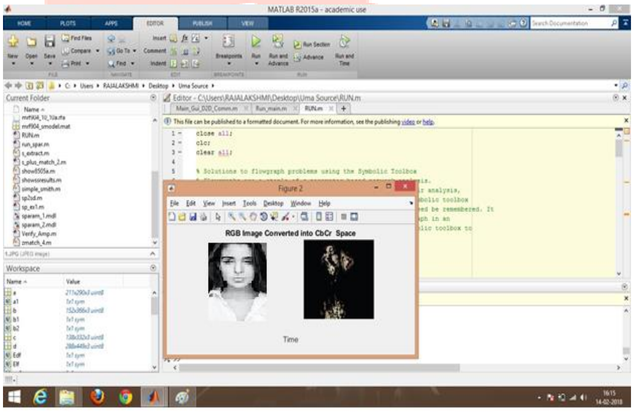


Fig 8: Input Image of Raw bits

It is made by the parasite Sphaerulina oryzina (syn. Cercospora Jan Sena, Cercospora India). The run of the mill twisted on leaves and upper leaves are light to dull dark colored, straight, and advance parallel to the vein. They are normally 2–10 millimeter long and 1–1.5 millimeter wide as appeared in Wounds on the leaves of profoundly powerless assortments may expand and interface together that shaping dark colored direct necrotic areas. Dark colored injuries are additionally found on pedicels. The sickness additionally causes recoloring on the leaf sheath, implied as "net smudge" due to the netlike example of dark colored and light darker to yellow zones. Thin dark colored spot can be mixed up for white leaf.


MATLAB R2015a - academic use
HOME
PLOTS
APPS
EDITOR
PUBLISH
VIEW
Current Folder
Workspace
Name
Value
Editor - C:\Users\RAJALAKSHMI\Desktop\Uma Source\RUN.m
Main_Gui_D2D_Comm.m
Run_main.m
RUN.m
Figure 2
File Edit View Insert Tools Desktop Window Help
RGB Image Converted into CbCr Space
Time

```
close all;
clc;
clear all;
% Solution to flowgraph problems using the Symbolic Toolbox
```

Fig 9: Face detection and Cbcr space analysis

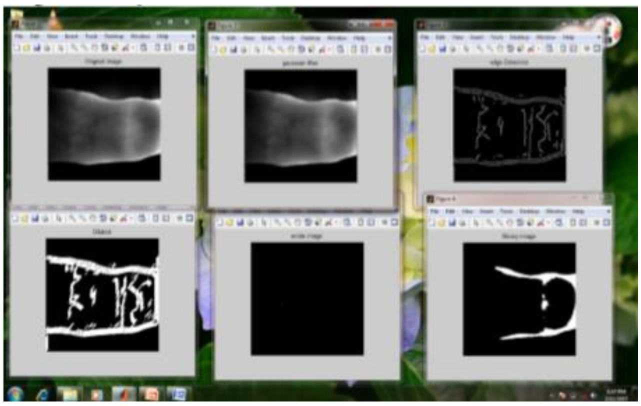


Fig 10: Fingerprint detection based on cropped image

Thinning is the transformation of a numerical image into a simplified, but topologically equivalent image. It is a kind of topological skeleton, but computed using numerical morphology operators. Thinning operation is determined by interpreting the origin of the structuring element to every possible pixel position in the image, and at each such position contrasting it with the basic image pixels. If the foreground and background pixels in the arranging element exactly match foreground and background pixels in the image, then the image pixel beneath the origin of the arranging element is set to background (zero). Otherwise it is left unaltered. Note that the structuring element must always have a one or a blank at its origin if it is to have any effect. The decision of structuring element determines under what situations a foreground pixel will be set to background, and hence it decides the submission for the thinning operation. A binary image can be stored in memory as a bitmap, a packed array of bits. A 640×480 image requires 37.5 KB of storage. Because of the small size of the image files, fax machine and document management solutions usually use this format. Most binary images also compress well with simple run-length compression patterns. Binary images can be interpreted as subsets of the two-dimensional integer lattice Z2; the field of morphological image processing was largely inspired by this view.

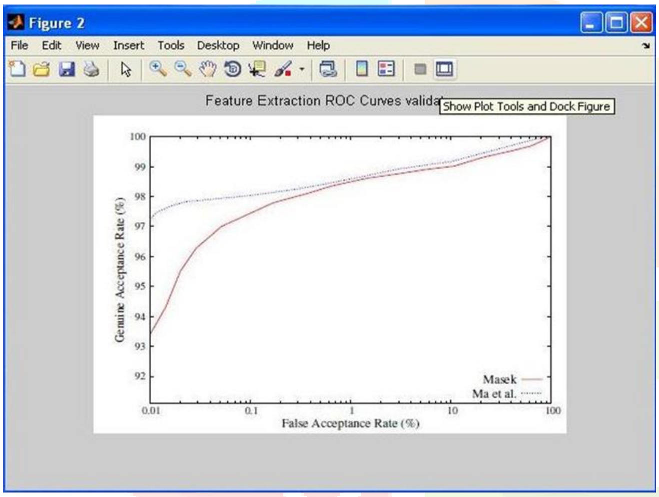


Fig 11: Feature Extraction Roc Curves Validates

The MASEK feature extraction algorithm combined with different classifier kernel functions (linear, or radial basis function (rbf), and polynomial), obtained experimental results showed the best precision with the rbf kernel (100%) and almost catches all the number of positive class even better than results. These figures show that for any given false positive rate, the true positive rate provided that, the test is outstanding. Comparing between the MASEK and Ma et, Al. feature extraction procedures by implementing a linear kernel function of the classier.

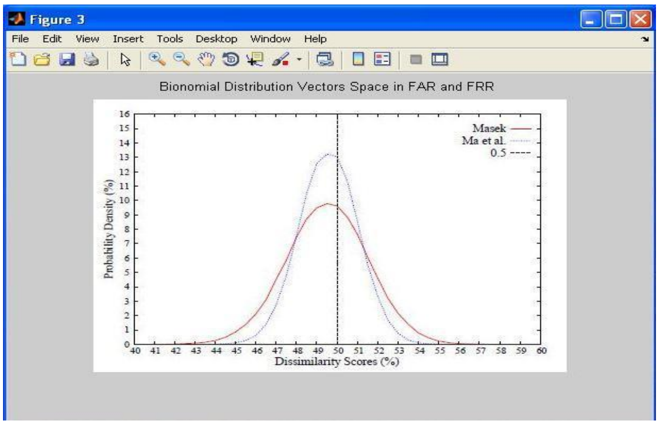


Fig 12: Binomial Distribution vector space in FAR and FRR

However, when applying radial basis kernel function with the Embedding with the MASEK feature extraction algorithm, this approach achieved its maximum detect ability rate. It can be determined that the MASEK using radial basis function with the MASEK feature extraction algorithm gives greater detect ability of the Tilapia species than the Ma et al. feature extraction algorithm. The context-based comparator obtains a slight improvement in accuracy requiring a complex calculation which may not be adequate in case biometric systems are run in identification mode. Best results are achieved for the reliability-driven comparator. In case of several authentication attempts user-specific reliability-masks 128 bit blocks (which require additional storage) are updated in order to reach a weighted comparison based on the most reliable bits in binary biometric feature vectors.

CONCLUSION

Encryption algorithm plays a significant role. The work proposed is to bring insight into the problem of biometric security. Innovative schemes were proposed for iris image and template protection which contains of two security layers. The primary layer is a strong watermarking algorithm which was executed to secure the reliability of the biometric image. In particular, an iris image that accommodates the authentication of a person is inserted in the digital image by randomly interchanging four pairs of the DCT middle band coefficients. The embedding locations were randomly selected based on a private key. Moreover, the proposed strength constants were included to add more robustness to the watermarking algorithm. However, the influence of watermarking attacks to iris watermark and the influence of watermarking embedding in Iris and face image are different for finger print recognition performance. In the first scenario, the watermarking attacks which lead to severe changes to face and iris watermarks cause a decrease on recognition performance. Feature Extraction Roc Curves Validates MASEK and Ma et, Al to obtain the false acceptance rate accurately. Distribution Reliability in Ma and MASEK is compared in the 128 bit blocks, and here it gives the accurate result on MASEK, is not clearly obtained in Ma. And it is determined that MASEK gives the accurate false acceptance rate for Authentication. However, the attacks which the embedding algorithm is robust to would not significantly affect recognition performance. The watermark inserting in the subsequent situation barely influences Finger print, iris and Face acknowledgment execution.

Future Enhancement

Essentially it is difficult to keep up the inventiveness of the input image is absolutely results to bending issues. So, a solid watermarking alongside cryptography can be made which can keep the image from being hacked just as misshaped. Generally, the file type as of now being worked upon for example .jpg configuration must to be improved to much more .gif, png design. Furthermore, last but not the least the encryption – unscrambling methods have to be changed according to improvement of latest advancements.

REFERENCES:

[1] P. Stavroulakis and M. Stamp, Handbook of Information and Communication Security. Springer, 2010.

[2] N. Ratha, J. Connell, and R. Bolle, "An Analysis of Minutiae Matching Strength" Springer Berlin Heidelberg, 2016, vol. 2091, book section 32, pp. 223–228.

[3] K. Martin, L. Haiping, F. M. Bui, K. N. Plataniotis, and D. Hatzinakos," A biometric encryption system for the self-exclusion scenario of face recognition," IEEE Systems Journal, vol. 3, no. 4, pp. 440–450, 2009.

[4] A. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," in 13th European Signal Processing Conference, EUSIPCO05, 2015, pp. 1–4.

[5] J. Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21–30,2004.

[6] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 385–395, 2011.

[7] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," Computer Vision and Image Understanding, vol. 117, no. 10, pp. 1512–1525, 2013.

[8] K. Park, D. Jeong, B. Kang and E. Lee, "A Study on Iris Feature Watermarking on Face Data" Springer Berlin Heidelberg, 2007, vol.4432, book section 47, pp. 415–423.

[9] A. Hassanien, A. Abraham, and C. Grosan, "Spiking neural network and wavelets for hiding iris data in digital images," Soft Computing, vol. 13, no. 4, pp. 401–416, 2009.

[10] S. Majumder, K. J. Devi, and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," IET Biometrics, vol. 2, no. 1, pp. 21–27, 2013.

[11] M. Paunwala and S. Patnaik, "Biometric template protection with DCT based watermarking," Machine Vision and Applications, vol. 25, no. 1, pp. 263–275, 2014.

[12] M. A. M. Abdullah, S. S. Dlay, and W. L. Woo, "Securing iris images with a robust watermarking algorithm based on Discrete Cosine Transform," in Proceedings of the 10th International Conference on Computer Vision Theory and Applications, vol. 3, 2015, pp. 108–114.

[13] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp.1081–1088, 2015.

[14] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Theoretical and practical boundaries of binary secure sketches," IEEE Transactions on Information Forensics and Security, vol. 3, no. 4, pp.673–683, 2008.

[15] S. Yan, Z. Xukai, E. Y. Du, and L. Feng, "Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method," IEEE Transactions on Computers, vol. 63, no. 4, pp. 902–916, 2014.