An Analysis of the Encryption Fusion Approach based on Face Recognition and Prime Numbers

Shinde Prashant Pandurang
Student of Department of Technology Savitribai
Phule University, Pune./Assistant Manager in
Deloitte for Cyber Risk Advisory Functions

ABSTRACT

Images play a significant role in various fields, such as biomedical, video conferencing, and remote sensing. Development in Digital Image Processing (IP) technology is motivated by the following key areas of application: improved human image awareness and processing of images for the recording and dissemination of machine perception. Two big problems are to be resolved if an image is to be transmitted. Firstly, the image may be accommodated within the specified bandwidth, and secondly, the image is protected. Image Encryption and Image Compression are 2 simple techniques in IP that are commonly utilized to satisfy the need for effective bandwidth usage and security. In this paper, An Encryption method by Fusion of Multi-Biometrics Data and Prime Numbers in which two algorithms postulations are identified with the Information Fusion techniques. First, one is FIF-Biometric and Numerical Information Fusion algorithm, which consolidates fingerprint and prime number to frame a hybrid fusion code. The second one is FIF, which consolidates face image code and a prime number to form a hybrid face code. The primary algorithm utilizes fingerprint as the biometric segment and the FIF algorithm utilizes a face image of the user. Then again fusion of fusion code of face and finger is managed using fif is applied to get the final output.

General Terms

Image processing, RSA Algorithm, Encryption.

Keywords

Face Recognition, image Encryption, image Cryptography, FIF.

1. INTRODUCTION

Face recognition (FR) technologies are a fraction of computing software for facial expressions & their importance in the field of research has recently increased. They use biometric knowledge from humans and quickly extend it to non-collaborative people rather than a signature, iris, fingerprint, etc. FR systems are commonly used & favored for people and safety cameras in metropolitan life. Some systems may be utilized for the detection of violence, video surveillance, and identification of people and associated protection operations. FR technology is a complex image processing challenge with complex lighting, occlusion, and shading on live images. This is a combination of techniques in IP and FR. To find a location of the faces in a given image, the detection application is used. The recognition algorithm is used in the detection of such images with known defined properties, typically found in most applications for computer vision. Form detection uses regular images, detects faces, and extracts facial features that include eyes, eyebrows, and nose [1].

In most cases the image is represented by pixels in the space domain; however, the frequency-domain representation obtained in the Fourier Transform is the most common one. Even from the perspective of object recognition the Fourier transformation of an image isn't quite insightful. Others such as wavelets, curvelets, contourlets, etc. provide patterns other than pixels or frequency as alternate representations. Such images are converted to promote the recognition of images. In this chapter, so present a survey of the literature on face recognition from still intensity images [2]. Face-recognition in human-computer interaction is a very relevant research content. It is used widely for secure networks and everyday life due to the benefit of the easy and non-contact acquisition. At a similar time, extracted features play the main role in facial recognition therefore scientists recommend certain forms of algorithms for extraction. Any three types of facial recognition strategies are available:

1) **An approach basing on local face feature recognition:** These algos for example have strong anti-interference and good rotation and explanatory variability, LDP (Local Derivative Pattern) & Local Binary Patches (LBP).

2) **An approach basing on global faces feature recognition:** For example, the Component Analysis Linear Discriminate Analytical Theory is therefore more recognizable local face algos than global algos in FR.

3) **An approach basing on fusing global face feature & local face feature:** For example Eye fusion, Noise feature extraction, Eigenfaces, etc.

2. IMAGE ENCRYPTION (IE)

Multimedia, Inter-net, telemedical, medical imaging, & military communication use image encryption. The level of security, the speed, and the resultant scale of the stream is nevertheless challenging. Although a chaotic system's dynamic reaction may be adaptable to initial values, chaotic system parameters, increasing numbers of researchers use chaotic sequences to encrypt images to secure their communication. The first-order chaotic scheme for encrypting digital images is a simple and fast method [3].

2.1 IE Algorithm

2 approaches are used to encrypt an image here.

2.1.1 Chaotic Mapping

Essentially, after a given algorithm, it marks the images and the original image may be recovered when reversed. The left-map reveals that the image first is a pixel line and is then shuffled with another algorithm and transformed again to N × N (encrypted). It is separated diagonally into two maps. This is seen from the N×N image.

2.1.2 Bit Plane Mixing

The square image includes N × N pixels of the L gray level. Every pixel A has a Gray Level value that can be seen as binary numbers.

$$A = Sum_{i=1}^{i=8} K_i * 2^i$$

While the image can be separated into 8 layers. The lowest binary numbers for image values are composed, as seen in the first layer; the second layer consists of the two coefficients, etc.

3. CRYPTOGRAPHY

Cryptography is an important multimedia content protection tool. Before being distributed through the internet, all multimedia files are encrypted. Because of file encryption, all entities without access to keys are useless. The key to content decryption will also not be revealed to anyone other than the service provider. There are other (symmetric) cryptography goals that can be accomplished, but three of the main objectives:

3.1 Confidentiality

It means that an adversary who has access to the communication channel is not able to get information about the content of messages swapped by communications partners.

3.2 Integrity

It ensures that the contents of the shared messages can not be updated unauthorized by an adversary having access to the contact link. In other terms, it stops an aggressive adversary from exploiting messages without recognizing the manipulation.

3.3 Authenticity

Encrypting is a way of shielding information against unwanted attacks by converting information to a shape that is not visible for attackers and ensuring an adversary who accesses a contact channel cannot alter the information regarding the origin of the transmitted messages. Data encryption primarily modifies data such as text; photograph, audio ... so that during transmission it becomes unreadable, invisible, or impenetrable. But the receptor only reverses key encryption known as key decryption to retrieve the original data.

Measurement of BNIF (Biometric & Numerical Information Fusion) is to add finger code with the figure section to establish an entrance key for safe commerce of benchmarks relevant to electronic currency. During the meantime, it reveals once again the critical moments of the method, which make the combination of knowledge possible:

1. RSA: to make code of number & private key;

2. Fingerprint Calculation: It is to separating biometric code;

3. This is to data mix articulations.

4. LITERATURE REVIEW

[3] The goal of this research has been to develop a new method that can be used for encrypting images to significantly increase security. To solve this question of image protection, so propose a distributed homomorphic imaging system, with representations of the visible electromagnetic spectrum of interest. In our encryption process, the red green blue (RGB) image is first divided into its channel images and the pixel numerical intensity value for each channel is written into several sub-values of less pixel intensity which means that for each pixel R, G, and B channel images, multiple component images are generated. The homomorphic encryption function enables each sub value for the pixel intensity to be encrypted separately by using an encryption key in every component image which leads to a distributed image encryption approach. Until transmission and/or storage, each encrypted part image may be compressed.

[4] Biological sequences are also utilized to encode data because of its features inherent in the implementation of cryptographic algorithms. DNA encryption is the most frequently utilized data authentication approach based on biological sequence characteristics. A new two-stage technique is introduced in this research to protect the images from unauthorized access. The enhancement of the protection is based on DNA Encryption & PCR (polymerase chain reaction). The suggested approach is evaluated using normal parameters to demonstrate the algorithm's efficiency.

[5] To place the human eye in multiple databases by pre-processing, ASEF Human Eye Location Algorithm has been implemented. Clustering also is then utilized to cluster face to gesture recognition. FR in all aspects of social life has been used increasingly in current years. FR also involves a range of similar strategies to construct facial recognition networks, including image retrieval, face location, preprocessing of facial expression, identity authentication, and identity search. Many face recognition systems today, though, have tremendous demands on the face and are very weak in their robustness. Multi-pose face recognition has, therefore, become a significant FR phenomenon.

[6] Encryption and time decryption of various algos of random data packets size have been observed. Next, this paper discusses the fundamental principles of cryptography: encryption & decoding. Secondly, very common RSA algos are compared to ECC (Elliptic Curve and El-Gamal). Our evaluation depends upon the length of key measurements that affects runtime. At last, our study ends by reflecting on various results between RSA & elliptical curve algorithms. Security of the Internet and privacy security for all users should be assured. Safety is also a significant issue when communication is exposed to networks. The information is rarely properly safeguarded in the world today as it should be. Cryptography is one of Network Security's most effective and effective elements. Cryptography is a system for the transmission of unintelligible information, which guarantees safe & secure communication among the sender & receiver. The sender can only decode information received & encoded by the approved receiver. Cryptography plays a key role in ensuring these networks are secure.

[7] The technique of DNA encoding and self- adaptive permutation was effective and efficient. The basic image is initially encrypted by DNA encryption in the DNA sequence. 1D chaotic map & LFSR (Linear Feedback Shift Register) produce the main series. The main sequence is used to block the encoded DNA image by complement it. The DNA inclusion law is then extended based on the chaotic map of two 1D. Eventually, a self-adaptive permutation technology is implemented using the image encoded disruption value. A decoded image may be completed with a reverse encryption method. Discussions & Results indicate the suggested approach has produced more effective encrypted images and thus improved statistical attack resistance.

[8] proposed an algorithm for human facial recognition merging algorithm for skin color identification with an algorithm for binary morphological examination. To that the

effect of illumination on the picture, firstly, captured images must go by YCrCb model recognition. For decreasing the impact of lighting on the image, HSV model recognition algo is approved. The obtained detection signal is converted into a binary image. The denotation of binary morphology would also take place, obtaining an image of human face recognition. Recent findings reveal that for uncomplicated human face images, a fairly difficult human face image & complicated human face images, algorithm introduced in this work will achieve detection and recognition rate of 90%, 93.3%, and 98.6%, respectively.

[9] Discussed is a technique that incorporates encryption and steganography to provide multilayer protection. A higher degree of protection is given by the proposed RSA cryptography algorithm combined with the dual audio algorithm. In our day-to-day activities, millions of people using the Internet. The protection of data security is very important for numerous commercial and non-commercial applications. Automated data security tools are therefore needed. Another significant thing is the reliability of network connectivity with the implementation of distributed computing systems. The distribution networks are used for the handling of data for both research institutions, businesses, and government organizations. The security of data during communication within a computer network at various locations where end-users concurrently operate was therefore unavoidable.

[10] The algorithm presented is based upon the RGB image fusion, but the color filters array dependent upon most generally used color in an array is Bayer image format, and most data processing and camera devices, however, are not the RGB model. This paper primarily extends a BAYER model based on fusion algorithms. In regular deviation, spatial frequency & information entropy, a new algorithm is superior to RGB. Bayer's algorithm is less than RGB's according to the test sum.

[11] Explanation of image fusion principle using hybrid medical multimodality images Together with CT, MRI, and cell activity in the body, structural features such as PET are significant for study. This work, therefore, demonstrates a synthesis of representations of PET & CT. The most commonly used image fusion algorithms are DWT (Discrete Wavelet Transformation), SWT (Stationary Wavelet Transforming), DCT (Discrete Curve Transformation), and main component analysis. The hybrid algorithm is developed with the incorporation of traditional and advanced fusion methods for overcoming demerits and improving image processing properties various algorithms are observed, investigated & compared by PSNR, ENTROPY & MSE efficiency.

RESEARCH GAP

- Enhancements on image pre-processing technologies, consisting of feature extraction [13].
- Efficient face recognition algorithms have developed rapidly over the last decade. Traditional face recognition algorithms may be categorized into 2 categories: holistic & local methods to characteristics.
- A neural network with radial bases with a non-negative matrix factorization is described in [14]. Facial recognition Furthermore, checking of the expression and speech,
- Wavelets from Gabor have been commonly used to describe the face by researchers who identify the face and features are known as a better representation of the face in terms of (rank-1) recognition rate [15].
- Further work will concentrate on expanding facial characteristics to more reliably identify faces [16].
- Besides, this application will be used to identify the medical images to determine the right disease previously confirmed [17].
- Chosen to reduce the number and inefficiency of dimensions only the most commonly used values of any encryption algorithm.

5. PROPOSE METHODOLOGY

In the extensive use, look at two algorithms postulations are identified with the Information Fusion techniques. First, one is FIF-Biometric and Numerical Information Fusion algorithm, which consolidates fingerprint and prime number to frame a hybrid fusion code. The second one is FIF, which consolidates face image code and a prime number to form a hybrid face code. Here look at two algorithms named FIF and FIF algorithms. Those depend on the Information Fusion techniques including physiological biometrics, for example, face recognition and fingerprint. The primary algorithm utilizes fingerprint as the biometric segment and the FIF algorithm utilizes a face image of the user. Then again fusion of fusion code of face and finger is managed using five is applied to get the final output. This code would be connected with the Hybrid code and would, therefore, allow you to use the second code if you lost the first.

5.1 Face Finger Information Fusion

This Algorithm is to connect the face image of the user & a bit data to form one of kind unique vector [12].

The plan is partitioned into three sections:

- Face Algorithm: it is segmented for separating biometric code;
- RSA: RSA is segmented to creating number code and private key;
- Fingerprint Algorithm: This algorithm is to separating biometric code;
- FIF Algorithm: it is part of the information combination.

Next, upload a real customer's photograph and convert it into a facial file. The biometric highlight of the image utilized by hybrid face code is differentiated by the SIFT algorithm. At this point, a bit of information is inputted and a stable RSA algorithm is used to obtain a private key & module vector. Strengthen face code and module vector and private key from bit data at that level. Place Face Information Fusion (FIF) algorithm for the hybrid fusion matrix. For transforming 2 vectors into a matrix that incorporates face code, module & private key vectors FIF algorithm is used. As an entranceway, the hybrid fusion vector can also be used.

Then the finger image was uploaded and converted into a finger code. The biometric highlights of the image used for the hybrid finger code are isolated by the SIFT algorithm. SIFT is a computer vision algorithm to identify and explain the local features of an image. FIF algorithm used to convert two vectors into a finger code, module, and private key vector matrix. As an entranceway, the hybrid fusion vector can also be used.

5.2 Face Information Fusion Algorithm

The FIF algorithm stages are specified below:

Be a, b € Z, 2 vectors, where a includes biometric element & b product of 2 prime no.

- Be s € Z: s=a + b; where a & b are sizes of biometric vector & module vector.
- Be q € Z: q= [v s] whole no. including s root.
- Nz1 = q- (a.q) and nz2 = q- (b.q) to reduce size of 2 vectors by.
- Original size of vectors is set by, a1 = a+bz1 & b1 =b+bz1.
- Additionally, categorize every vector into blocks which would be hybrid vector lines, vector including 2 vectors added incorrect way, nbloocc_a1 = m1/q,& nbloocc_a1 = b1/q.
- Be: P ed = bz1 + bz2,
- A private key is used to insert the blocks; the no for 1st part of the private key specifies no. of vector blocks to be inserted in a hybrid matrix, & the second private key component defines several blocks of module vector to be inserted into vector hybrid, etc.
- At last, algo has to confirm that got matrix is squared as,

PedTot = q2 - (a + b),

Dif = P ed – PedTot

Then, 3 cases can be notable:

Dif < 0 =⇒ line totaling,

Dif = 0 =⇒ no added padding,

Dif > 0 =⇒ column totaling.

5.3 Finger Information Fusion Algorithm

The numeric size vectors in the FIF algorithm include fingerprint code, node, and private key. The fingerprint, module, and private key vectors are generated by the FIF algorithm to be padded. The vector span must be evened out for the padding process.

The transformation of two vectors by FIF algorithm into one vector takes place below:

- Be a & b € Z, a & b are 2 vectors, wherever includes biometric element & b product of 2 prime numbers.
- Be s € Z: s = a +b; a whole no. including s root.
- To have a square root, this is the need that bz1= q-mod (a .q) and bz1= q-mod (b .q).
- Hence original dimensions of vectors would be: a1 = a+az1 & b1 =b+bz1.
- Categorize every vector into blocks that would be dual vector lines, a vector that includes 2 inserted vectors correctly,
- Be: Ped = bz1 + bz2,
- A private key is used to insert the blocks; the no for 1st part of the private key specifies the number of vector blocks to be inserted in a hybrid matrix, and 2nd private key part defines several blocks of matrix module to be inserted into vector hybrid, etc.
- The algorithm will eventually check that matrix obtained is genuinely squared as,

PedTot = q2 - (a + b),

Dif = P ed – PedTot

- after that, 3 cases may be imminent:

Dif < 0 =⇒ totaling of a line,

Dif = 0 =⇒ no added padding,

Dif> 0 =⇒ totaling of a column.

1) Be a, b € Z, 2 vectors, where a includes biometric element & b product of 2 prime no.

2) Be s € Z: s=a + b; where a and b are the sizes of biometric vector & module vector.

3) Be q € Z: q= [√ s] a whole no. including s root.

4) To decrease size of 2 vectors by, nz1 = q-mod (a. q) & nz2 = q-mod (b. q).

5) Original size of vectors is specified by, a1 = a+bz1 & n1 =n+nz1.

6) Besides, separate each vector in blocks which would be hybrid vector lines, a vector including 2 vectors inserted suitably, bloocc_a1 = a1/q, and bloocc_b1 = b1/q.

7) Be: P ed = bz1 + bz2,

8) The private key is provided to insert blocks; 1st component in a private key is specified by no. of blocks inserted in a hybrid vector of face code, & 2nd component in private key defines numbers of blocks inserted into a vector of the hybrid vector.

9) Algorithm will eventually show that matrix is simply squared, PedTot = q2 − (a + b), Dif = P ed – PedTot So you may discern three cases: diff < 0 =⇒ inserting a line, Dif = 0 =⇒ no inserting padding, Dif > 0 = ⇒ adding a column. Padding line or column generated with a private key.

10) While you produce a squared Union U matrix, the grid U & permutation matrix P is after that, you now have transitioned in parts. The personal key of estimation cryptography chooses the permutation matrix. A structure of six 3×3 change frames, which is computed like those of matrix U, is generated from a common grid:

11) Finally, you must have the outcome of the Union Matrix U and the P frameworks permutation: F = UP 12) you can receive a Fusion-F structure segregated by the method to generate the V-vector ranking which is hybrid-face code.

6. FLOW DIAGRAM OF PROPOSED WORK

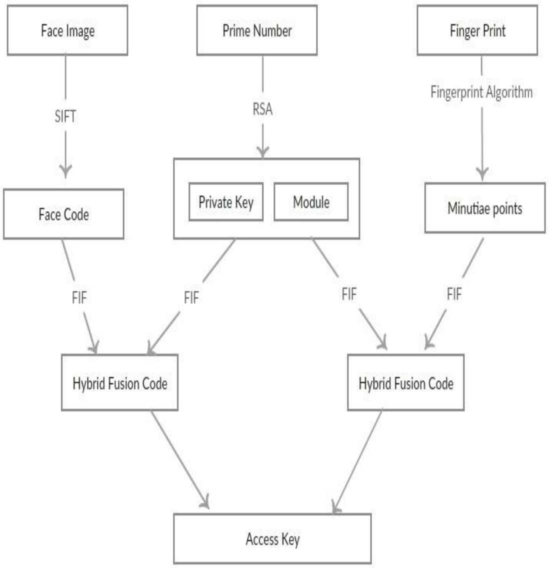
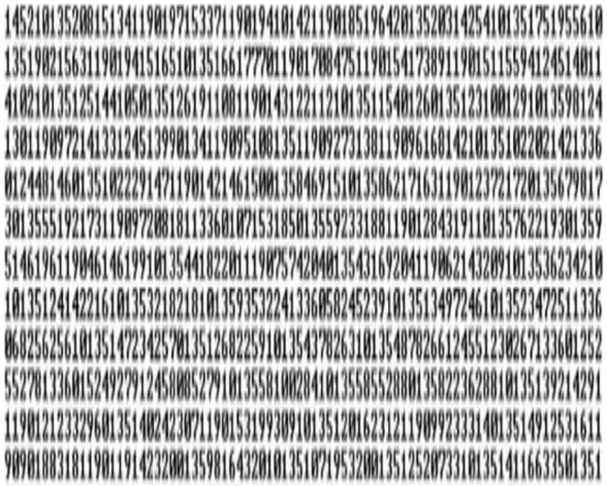


Fig 1: If necessary, the images can be extended both columns

7. EXPERIMENTAL RESULTS

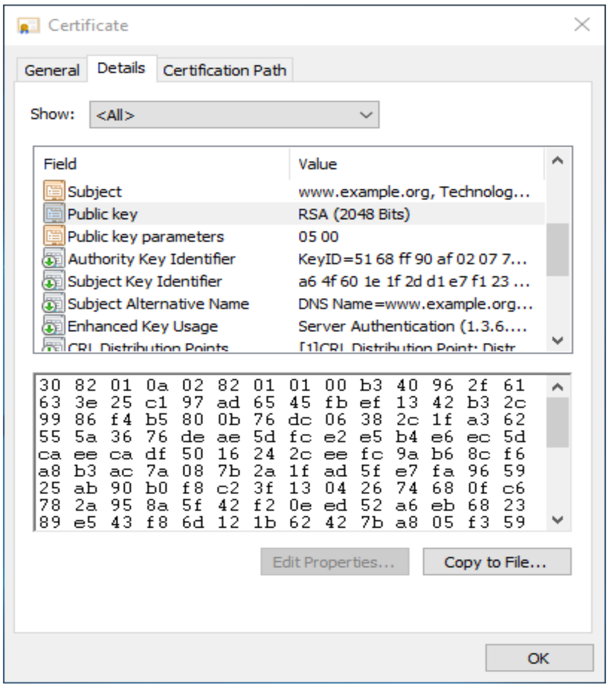
By using MATLAB as a simulation tool for our experimental analysis and java 7. A category of uses called toolboxes is illustrated by MATLAB. To encourage many users to research and concern MATLAB, toolboxes encourage you to specialize in technologies. This section has discussed the experimental findings of the suggested solution. Matlab follows the proposed solution. The suggested solution has been checked for various Face sets. In order to generate the V-vector output, a hybrid face code, the Fusion F structure we know must be divided. Numerous experiments were carried out on several images of iris and fingerprints that led to certain domain parameters for each images and private keys. With different sets of fingerprints & face the proposed method was checked



```
14521013520815134119019715337119019410142119018519642013520314254101351751955610
13519021563119019415165101351661777011901708475119015417389119015115594124514011
41021013512514410501351261911001190143122112101351154012601351231001291013598124
13011909721413312451399013411909510013511909273130119096160142101351022021421336
01244014601351022291471190142146150013504691510135062171631190123721720135679017
30135551921731190972081811336010715318501355923318811901284319110135762219301359
51461961190461461991013544182201119075742040135431692041190621432091013536234210
10135124142216101353218218101359353224133605824523910135134972461013523472511336
06825625610135147234257013512682259101354378263101354878266124551230267133601252
55270133601524927912450085279101355810028410135585528001358223628810135139214291
11901212332960135140242307119015319930910135120162312119099233314013514912531611
90901883181190119142320013598164320101351071953200135125207331013514116633501351
```

Fig 2: Face Code

The correspondent of a face code Figure 2 as a numerical vector shows in the above figure



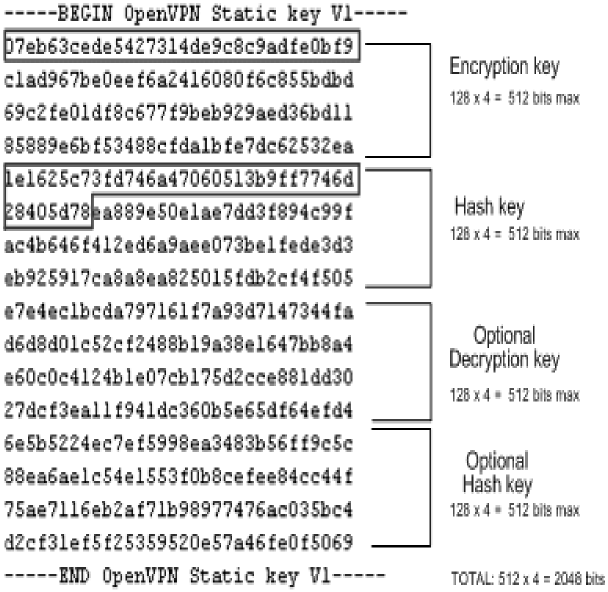
Show: <All>

Field	Value
Subject	www.example.org, Technolog...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=51 68 ff 90 af 02 07 7...
Subject Key Identifier	a6 4f 60 1e 1f 2d d1 e7 f1 23 ...
Subject Alternative Name	DNS Name=www.example.org...
Enhanced Key Usage	Server Authentication (1.3.6....
CRL Distribution Points	[1]CRL Distribution Point: Distr

```
30 82 01 0a 02 82 01 01 00 b3 40 96 2f 61
63 3e 25 c1 97 ad 65 45 fb ef 13 42 b3 2c
99 86 f4 b5 80 0b 76 dc 06 38 2c 1f a3 62
55 5a 36 76 de ae 5d fc e2 e5 b4 e6 ec 5d
ca ee ca df 50 16 24 2c ee fc 9a b6 8c f6
a8 b3 ac 7a 08 7b 2a 1f ad 5f e7 fa 96 59
25 ab 90 b0 f8 c2 3f 13 04 26 74 68 0f c6
78 2a 95 8a 5f 42 f2 0e ed 52 a6 eb 68 23
89 e5 43 f8 6d 12 1b 62 42 7b a8 05 f3 59
```

Fig 3: Product of 2 prime numbers (Module)

The above figure illustrates why mathematics and informatics are not able to construct a number by even attempting any combination. It's so important to consider. It implies that first attempts are made to crack in two, then in three, then in four, etc. If you try to fasten a primary number, particularly a very high number, you have (essentially) to try every possible number of two. The primary numbers used for cryptography take years (even hundreds) in the fastest computers.



```
-----BEGIN OpenVPN Static key V1-----
07eb63cede5427314de9c8c9adfe0bf9
c1ad967be0eef6a2416080f6c855bdbd
69c2fe01df8c677f9beb929aed36bd11
85889e6bf53488cfda1bfe7dc62532ea
1e1625c73fd746a47060513b9ff7746d
28405d78ea889e50e1ae7dd3f894c99f
ac4b646f412ed6a9aee073be1fede3d3
eb925917ca8a8ea825015fdb2cf4f505
e7e4ec1bcda797161f7a93d7147344fa
d6d8d01c52cf2488b19a38e1647bb8a4
e60c0c4124b1e07cb175d2cce881dd30
27dcf3ea11f941dc360b5e65df64efd4
6e5b5224ec7ef5998ea3483b56ff9c5c
88ea6ae1c54e1553f0b8cefee84cc44f
75ae7116eb2af71b98977476ac035bc4
d2cf31ef5f25359520e57a46fe0f5069
-----END OpenVPN Static key V1-----
```

Fig 4: Private Key

The figure above indicates that personal key encryption uses a single key to both ciphertext and plaintext encoding. The sender and the receiver themselves will share the key and this key method for exchanging information is a complete subject of cryptography.

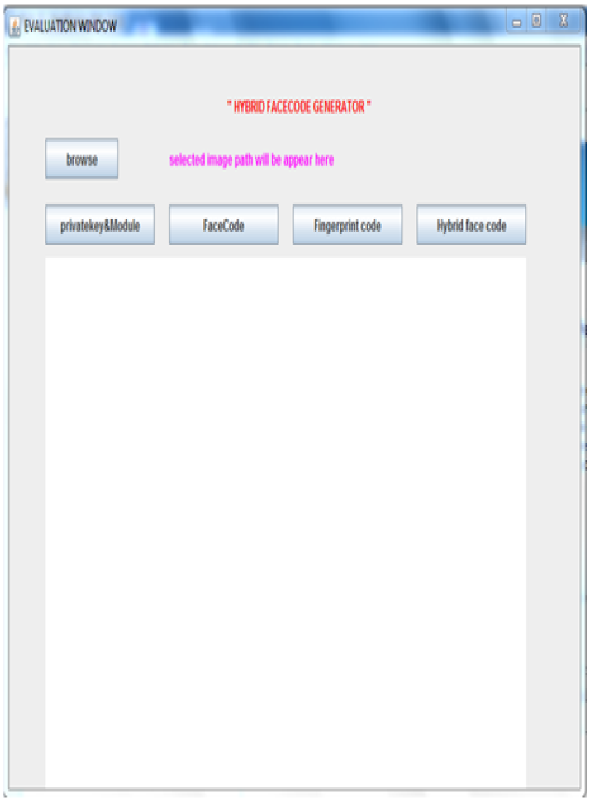
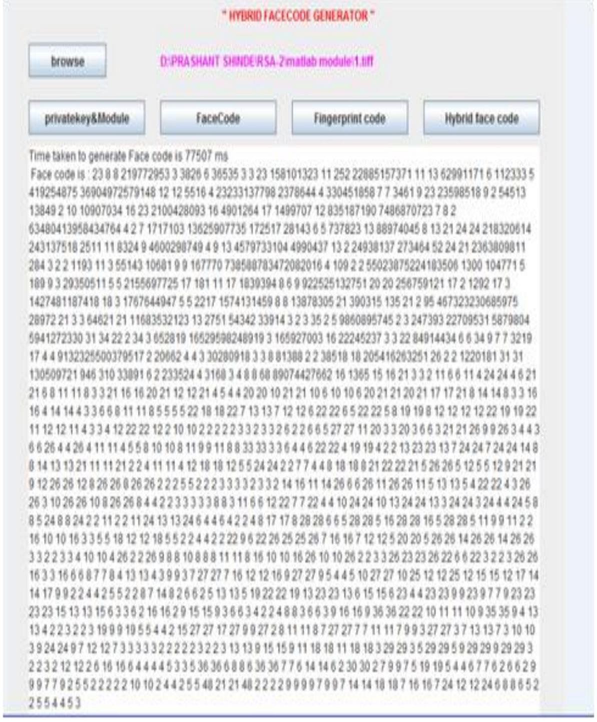


Fig 5: Show the starting point to browse image

Figure 5 shows the basic points for browsing image


* HYBRID FACECODE GENERATOR *
browse
D:PRASHANT SHINDE\RSA-2\matlab module\1.tiff
privatekey&Module
FaceCode
Fingerprint code
Hybrid face code

```
Time taken to generate Face code is 77507 ms
 Face code is : 23 8 8 219772953 3 3826 6 36535 3 3 23 158101323 11 252 22885157371 11 13 62991171 6 112333 5
419254875 36904972579148 12 12 5516 4 23233137798 2378644 4 330451858 7 7 3461 9 23 23598518 9 2 54513
13849 2 10 10907034 16 23 2100428093 16 4901264 17 1499707 12 835187190 7486870723 7 8 2
6348041395843476 4 4 2 7 1717103 13625907735 172517 28143 6 5 737823 13 88974045 8 13 21 24 24 218320614
243137518 2511 11 8324 9 4600298749 4 9 13 4579733104 4990437 13 2 24938137 273464 52 24 21 2363809811
284 3 2 2 1193 11 3 55143 10681 9 9 167770 7385887834720820164 4 109 2 2 5502387522418350 6 1300 104771 5
189 9 3 29350511 5 5 2155697725 17 181 11 17 1839394 8 6 9 922525132751 20 20 256759121 17 2 1292 17 3
1427481187418 18 3 1767644947 5 5 2217 1574131459 8 8 13878305 21 390315 135 21 2 95 467323230685975
28972 21 3 3 64621 21 11683532123 13 2751 54342 33914 3 2 3 35 2 5 9860895745 2 3 247393 22709531 5879804
5941272330 31 34 22 2 34 3 652819 165295982489193 165927003 16 22245237 3 3 22 84914434 6 6 34 9 7 7 3219
17 4 4 913232550037951 7 2 20662 4 4 3 30280918 3 3 8 81388 2 2 38518 18 205416263251 26 2 2 1220181 31 31
130509721 946 310 33891 6 2 233524 4 3168 3 4 8 8 68 89074427662 16 1365 15 16 21 3 3 2 11 6 6 11 4 24 24 4 6 21
21 6 8 11 11 8 3 3 21 16 16 20 21 12 12 21 4 5 4 4 20 20 10 21 21 10 6 10 10 6 20 21 21 20 21 17 17 21 8 14 14 8 3 3 16
16 4 14 14 4 3 3 6 6 8 11 11 8 5 5 5 5 22 18 18 22 7 13 13 7 12 12 6 22 22 6 5 22 22 5 8 19 19 8 12 12 12 12 22 19 19 22
11 12 12 11 4 3 3 4 12 22 22 12 2 10 10 2 2 2 2 2 3 3 2 3 3 2 6 2 2 6 6 5 27 27 11 20 3 3 20 3 6 6 3 21 21 26 9 9 26 3 4 4 3
6 6 26 4 4 26 4 11 11 4 5 5 8 10 10 8 11 9 9 11 8 8 33 33 3 3 6 4 4 6 22 22 4 19 19 4 2 2 13 23 23 13 7 24 24 7 24 24 14 8
8 14 13 13 21 11 11 21 2 2 4 11 11 4 12 18 18 12 5 5 24 24 2 2 7 7 4 4 8 18 18 8 21 22 22 21 5 26 26 5 12 5 5 12 9 21 21
9 12 26 26 12 8 26 26 8 26 26 2 2 2 5 5 2 2 2 3 3 3 3 2 3 3 2 14 16 11 14 26 6 6 26 11 26 26 11 5 13 13 5 4 22 22 4 3 26
26 3 10 26 26 10 8 26 26 8 4 4 2 2 3 3 3 3 3 8 8 3 11 6 6 12 22 7 7 22 4 4 10 24 24 10 13 24 24 13 3 24 24 3 24 4 4 24 5 8
8 5 24 8 8 24 2 2 11 2 2 11 24 13 13 24 6 4 4 6 4 2 2 4 8 17 17 8 28 28 6 6 5 28 28 5 16 28 28 16 5 28 28 5 11 9 9 11 2 2
16 10 10 16 3 3 5 5 18 12 12 18 5 5 2 2 4 4 2 2 22 9 6 22 26 25 25 26 7 16 16 7 12 12 5 20 20 5 26 26 14 26 26 14 26 26
3 3 2 2 3 3 4 10 10 4 26 2 2 26 9 8 8 10 8 8 8 11 11 8 16 10 10 16 26 10 10 26 2 2 3 3 26 23 23 26 22 6 6 22 3 2 2 3 26 26
16 3 3 16 6 6 8 7 7 8 4 13 13 4 3 9 9 3 7 27 27 7 16 12 12 16 9 27 27 9 5 4 4 5 10 27 27 10 25 12 12 25 12 15 15 12 17 14
14 17 9 9 2 2 4 4 2 5 5 2 2 8 7 14 8 2 6 6 2 5 13 13 5 19 22 22 19 13 23 23 13 6 15 15 6 23 4 4 23 23 9 9 23 9 7 7 9 23 23
23 23 15 13 13 15 6 3 3 6 2 16 16 2 9 15 15 9 3 6 6 3 4 2 2 4 8 8 3 6 6 3 9 16 16 9 36 36 22 22 10 11 11 10 9 35 35 9 4 13
13 4 2 2 3 2 2 3 19 9 9 19 5 5 4 4 2 15 27 27 17 27 9 9 27 2 8 11 11 8 7 27 27 7 7 11 11 7 9 9 3 27 27 3 7 13 13 7 3 10 10
3 9 24 24 9 7 12 12 7 3 3 3 3 3 2 2 2 2 2 3 2 2 3 13 13 9 15 15 9 11 18 18 11 18 18 3 29 29 3 5 29 29 5 9 29 29 9 29 29 3
2 2 3 2 12 12 2 6 16 16 6 4 4 4 4 5 3 3 5 36 36 6 8 8 6 36 36 7 7 6 14 14 6 2 30 30 2 7 9 9 7 5 19 19 5 4 4 6 7 7 6 2 6 6 2 9
9 9 7 7 9 2 5 5 2 2 2 2 2 10 10 2 4 4 2 5 5 48 21 21 48 2 2 2 2 9 9 9 9 7 9 9 7 14 14 18 18 7 16 16 7 24 12 12 24 6 8 8 6 5 2
2 5 5 4 4 5 3
```

Fig 6: Fusion of Multibiometrics

Multibiometrics are spoofing resistant and have a small FAQ. Multi-biometrics, however, require storing a number of biometric models for each user, thereby raising the risk of user privacy and protection. The multibiometric fusion in Figure 6 reveals .

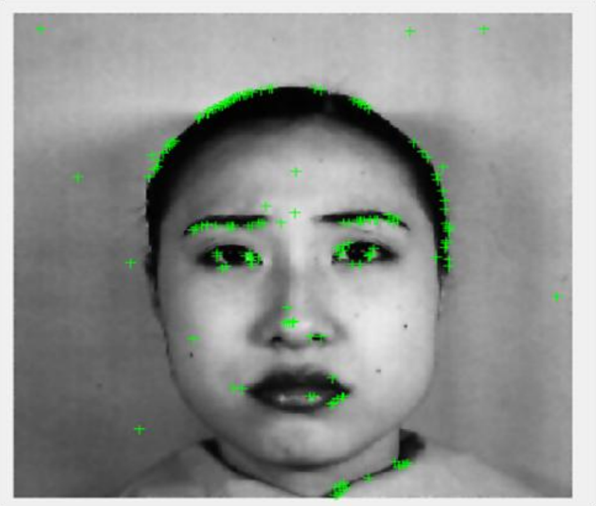


Fig 7: Biometric Authentication using Face Recognition

Due to its uniqueness and its strength, this figure shows the key attribute for bio authentication in the past few years. There was a mistake. By analyzing colored skins in the facial image, the proposed method estimates the face. The face edge characteristics of the identified face skeleton are then removed.

Table 1. Sample ECC parameters and Outputs

Keyword	Variable	Output
ECC Parameter s	P	7012
	A,B	5,4
	G	2916 4335
Keys	Private Key	219156166bdada660033e 23ed45gh
	Public Key A	5840c76d4a9c5c69222f87 e4ab23
	Public Key B	6e273782349b244a313899 Ad234d36
Encryption n and Decryption using ECC	Plain Text	Hi this is a message to encrypt
	Encrypted Text	ee90dc44eb4a7f5f66c09c3 1dce01e93
	Decrypted Text	Hi this is a message to encrypt

The table above shows various operations in the GF(P) elliptical curve regions, such as addition , multiplication, reverse-method, development of parameters, key generation, encryption and decryption.

8. CONCLUSION

By implementing an FFIF-algorithm called Hybrid Knowledge Fusion. Through combining through biometric human approaches, attempted to build a stable cryptographic key for improved protection. An important approach to the generation of stable, multimodal biometric cryptographic keys. FIF is a general principle that is fully independent of the biometric segment we find, which more than anything is reversible, but only if the biometric segment is additionally accessible to the private key generated by the open key cryptographic measurement. A conceivable application of this system of encryption is related to the confirmation of an individual. To specify encryption algorithms utilizing information fusion techniques with physiological biometrics and a numerical part. The last yield the hybrid fusion code contains the unique characteristics of the user (Fingerprint code, Face code), which is used as a character of the legal user. By utilizing a hybrid fusion vector, to a degree may keep away by attacks such as replay attacks, Phishing attacks, & brute force attacks, & may confirm that the user is legal or not. In this paper, we implement an expansion of the figured it out a calculation to multi-biometrics, to make it the most efficient it is feasible for the points we need. At last, to assess the efficiency, a benchmark will be planned to intend to give near outcomes as far as both figuring time and asset utilization.

9. FUTURE WORK

An expansion of the figured it out a calculation to multi-biometrics, to make it the most efficient it is feasible for the points we need. At last, to assess the efficiency, a benchmark will be planned in the future to give near outcomes as far as both figuring time and asset utilization. The suggested solution is to be applied to several distinctive biometric characteristics in future work. Quality metrics & partial face matching are presented & running time analysis is performed.

10. REFERENCES

[1] L. Zhi-fang, Y. Zhi-sheng, A.K.Jain and W. Yun-Xiong, 2003, “Face Detection And Facial Feature Extraction In Color Image”, Proc. The Fifth International Conference on Computational Intelligence and Multimedia Applications (ICCIMA’03), pp.126-130, Xi’an, China...

[2] Mohamed El Aroussi, “Information Fusion towards a Robust Face Recognition System”, research gate https://www.researchgate.net/publication/277201573 July 2009.

[3] M. I. Wade, M. Chouikha, T. Gill, W. Patterson, T. M. Washington, and J. Zeng, "Distributed Image Encryption Based On a Homomorphic Cryptographic Approach," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 2019, pp. 0686-0696.

[4] M. Roy et al., "A Dual Layer Image Encryption using Polymerase Chain Reaction Amplification and DNA Encryption," 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India, 2019, pp. 1-4.

[5] J. Li and D. Zhang, "Face gesture recognition based on clustering algorithm," 2019 Chinese Control And Decision Conference (CCDC), Nanchang, China, 2019, pp. 2008-2012.

[6] F. Mallouli, A. Hellal, N. Sharief Saeed and F. Abdulraheem Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 2019, pp. 173-176.

[7] I. Jain, S. A. Fattah, and C. Shahnaz, "Natural and Medical Image Encryption Using Self-Adaptive Permutation and DNA Encoding," 2018 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), Chonburi, Thailand, 2018, pp. 99-102.

[8] J. Wan and Y. Wang, "The Human Face Recognition Algorithm Based on the Improved Binary Morphology," 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, 2018, pp. 2625-2628.

[9] K. N. Bangera, N. V. S. Reddy, Y. Paddambail and G. Shivaprasad, "Multilayer security using RSA cryptography and dual audio steganography," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 492-495.

[10] H. Wang et al., "A new image fusion algorithm based on Bayer format," 2017 14th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, 2017, pp. 158-161.

[11] G. D. Patne, P. A. Phone, and K. R. Tuckley, "Review of CT and PET image fusion using hybrid algorithm," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, 2017, pp. 1-5.

[12] Gautham SEKAR, “Cryptanalysis and Design of Symmetric Cryptographic Algorithms”, Dissertation presented in partial fulfillment of Arenberg Doctoral School of Science, Engineering & Technology Faculty of Engineering Department of Electrical Engineering (ESAT) 2011.

[13] G.Iovane, L.Puccio, G.Lamponi, A.Amorosia. Electronic access key based on the innovative Information Fusion technique involving prime numbers and biometric data. Journal of discrete mathematical sciences and cryptography. Taru Publication, 2010.

[14] N. Ruggeri. Principles of pseudo-random number generation in cryptography, University of Chicago, 2006.

[15] G. Mary Amirtha Sagayee, S Arumugam, and G.S.Anandha Mala(2013), Biometric Encryption using Enhanced Finger Print Image and Elliptic Curve, IJCSNS, VOL.13 No.7, July 2013:106- 113.

[16] L. Hong, A. K. Jain and S. Pankanti, \Can multibiometrics improve performance?," in Proceedings AutoID'99, (Summit(NJ), USA), pp. 59{64, Oct 1999.

[17] G. Feng, D. Hu K. Dong, and D. Zhang, “When faces are combined with palmprints: A novel biometric fusion strategy”, pp. 332–341, 2004.