# Cancelable Biometrics Using Deep Learning

**Saloni[1], Subham Jain[2], K R Mamatha[3]**

*Student[1], Student[2], Assistant Professor[3]*
BMS College Of Engineering,Bangalore,India[1,2,3]

**Abstract—Biometric authentication technologies tend to be more usable than standard login and token-based verification solutions. Biometric technology, on the other side, raises a slew of privacy concerns. Biometrics are permanently associated with a person and cannot be changed. As a result, when a biometric information is hacked, it is lost forever, possibly for all apps that utilize it. Furthermore, if the same biometric is used across many applications, cross-matching biometric datasets might be used to track a person from one app to the next. To address these issues, we present numerous approaches for generating multiple cancelable identities from fingerprint photos in this study. By releasing a new transformation key, a user can receive large numbers biometric IDs and they will need. An ID can be terminated and replaced, if it is compromised. To accomplish revocability and avoid cross-matching of biometric datasets, we employed the Cartesian transformation technique with Reed Solomon error correction.**

**Keywords—Cancelable biometrics, revocable,fingerprint identification, image registration,privacy, security.**

## I. INTRODUCTION

Due to the increasing frequency of cyberattacks, personal identification numbers, tokens, and passwords have been shown to be completely insufficient for identity security. Biometric technologies have grown in popularity as a safe tool for user authentication during the last decade.In this study, to ensure the secrecy of biometric data, the 'Cancelable Biometrics' technique is used. Deep learning was used to construct a cancelable biometric system for multi-instance biometrics. The provided cancelable biometric system has a great verification accuracy, biometric template confidentiality and cancelability, short response times, and cost efficiency.

## II. LITERATURE SURVEY

Cancellable biometrics, according to Jiankun Hu et al. [1], is an essential biometric template protection solution that efficiently manages privacy and security problems when cached biometric templates are hijacked. This study describes a Hadamard transform-based method for developing cancelable fingerprint templates. Because the suggested cancelable templates are not orientated, fingerprint registration errors are avoided. The suggested method seeks to protect frequency domain binary string specimens since they include crucial details of the original fingerprint minutiae. The suggested partial Hadamard transform safeguards the frequency-domain samples of a binary string. They use a partial Hadamard matrix in their non-invertible transformation, which is easily built using a really random generated index vector. A susceptible template can be terminated and a replacement one produced by creating an alternate index vector. The experimental results indicate that the novel technique outperforms conventional sequence-free cancelable fingerprint templates.

NaliniK et.al[2] discussed that conventional password and token-based verification strategies have apparent usability

advantages over biometrics-based authentication systems. On the other hand, biometrics raises a plethora of privacy concerns. A biometric is linked to a user indefinitely and cannot be altered. As a result, if a biometric identification is compromised, it is permanently destroyed, potentially for all applications that rely on it. Moreover, if the same biometric is used in several platforms, cross-matching biometric databases may be able to track a person from one app to the next. To overcome these concerns, this paper shows many ways for producing several cancelable identities from fingerprint pictures. By releasing a new transformation "key," a user may be granted as many biometric IDs as they require. When the IDs are compromised, they can be terminated and replaced. The performance of several ways for altering microscopic places such as cartesian, polar, and surface folding transformations is investigated. Multiple investigations indicate that they can achieve revocability while also avoiding biometric dataset cross-matching. It is further demonstrated that the transfigures are noninvertible by showing that retrieving the original biometric identification from a changed form is computationally as difficult as guessing at random. The author proposes that feature-level cancelable biometric manufacturing is achievable in large biometric deployments based on these actual findings and theoretical study.

Harkeerat et.al[3] discussed that a cancelable biometric-based template preservation approach to address security and privacy problems that have arisen as a result of biometric systems' widespread use. Cancelable biometrics converts a user's biometric identification into a pseudo-biometric recognition that may be stored and matched. Pseudo-identity reduces privacy threats while also allowing for revocation in the event of a breach. This work introduces the random distance approach, a revolutionary template transformation strategy that not only creates discriminative and privacy-preserving revocable pseudo biometric IDs but also decreases their size by 50%. Extensive testing is carried out on unimodal and multimodal pseudo-identities created using multiple biometric categories such as face, To test identification and protection performance, thermal face, palm print and finger vein are used. In the worst-case scenario, the matching accuracy obtained with the suggested cancelable templates is comparable to that obtained in the original state.

Mohamed et al. [4] discussed a multi-biometric system that incorporates information from many biometric modalities to increase each biometric system's performance and make it more resistant to spoof attempts. The authors provide a secure multimodal biometric system based on multiple level fusion, which makes use of a convolution neural network (CNN) and a Q-Gaussian multi support vector machine (QG-MSVM). They created two authentication systems, each with its own set of level fusion algorithms: feature level fusion and decision level fusion. To extract characteristics for individual modalities, the CNN algorithm is employed. They chose two layers from CNN that had the best accuracy in this stage, and each layer is treated as an independent feature descriptor. The biometric templates were then created by combining them utilizing the suggested internal fusion. They then used one of the cancelable biometric approaches to safeguard these templates and improve the proposed system's security. To improve the efficacy of the authentication step, they used QG-MSVM as an authentication classifier. Their algorithms were put through their paces on a variety of publicly accessible ECG and fingerprint databases. According to the experimental results, the suggested multimodal techniques are more effective, resilient, and trustworthy than current multimodal authentication methods.

Jihyeon et.al [5] told that despite the fact that biometrics is considered a more reliable and user-friendly option for identity management than password- or token-based approaches, biometric templates are prone to adversary attacks, which might result in privacy invasion and permanent identity theft. Cancelable biometrics is a blueprint protection approach that uses a parameterized transformation method and user/application-specific parameters to create a noninvertible identifier from the original biometric template. However, the requirement to input parameters in ownership (token) or memory (password) form in conjunction with biometrics, thus two factors, jeopardize biometrics usage. They offer a one-factor cancellable biometric authentication technique for template protection based on Indexing First Order hashing, a custom-made locality sensitive hashing algorithm. They assess the proposed method against their template security design criteria, which include noninvertibility, renewability, unlikability, and correctness.

Xingbo et.al [6] discussed that when it comes to biometric template protection, cancelable biometrics (CB) mentions to an irreversibly yet similarity-preserving alteration on the initial template. The comparison between template/blueprint and query instance may be conducted in the transfigure domain without sacrificing accuracy performance because to the similarity preserving characteristic. Unfortunately, this attribute attracts a specific type of attack: similarity-based attacks (SA).SA creates a preimage that is the opposite of the altered template and can be utilized for imitation or cross-matching. They offer a Genetic Algorithm enabled similarity-based attack framework (GASAF) in this study to show that CB schemes with similarity preservation properties are extremely vulnerable to similarity-based attacks. A new set of measures is also being developed to assess the efficacy of the similarity-based approach. Thee test two representative CB systems: Bio Hashing and Bloom-filter, in this study. The findings of the experiment show that this form of assault is vulnerable.

Ming Jie, et al[7] presented an approach for medical photos where they have used an unique multimodal biometric-based encryption. The secret keys are created using the efficient and safe Advanced Encryption Standard Cipher Block Chaining (AES-CBC) encryption method and Indexing First One (IFO) hashing. The suggested solution employs biometrics such as the person's iris and fingerprint but rather than using the biometrics' characteristics effectively, they are hashed using the IFO process to generate a confidential key that can be annulled and regenerated in the event of a breach, assuring the biometrics' security. To encrypt the medical picture, the IFO hashes produced from the biometric feature vectors are employed as two distinct secret keys in a two-round AES-CBC method. The medical picture can be decrypted by running the AES-CBC rounds backwards with the proper keys, implying that only the right user will be allowed to decode the image with a high probability. This encryption approach improves on several current biometric-based medical encryption systems that don't consider the biometric template's security.

Tanuja et.al [8] talked about cloud computing, that it is a technology that has gained rapid popularity in recent years.It has made it possible to utilize massive processing power in a flexible and cost-effective manner. Biometric technology use in commercial and government enterprises is now routine security practise. Unconstrained biometric systems, on the other hand, are computationally and monetarily costly, particularly when user enrolment is substantial. A realistic approach would be to build a cloud-based biometric system that can be utilized as an authentication system everywhere. In this study, they present the first cancelable biometric architecture based on deep learning in the cloud. They demonstrate that the cloud is an excellent choice for biometric systems that demand extensive computing, fast reaction times, and great accuracy.

PM Benson et.al[9] discussed that the Internet of Things (IoT) is a new technology that connects electrical gadgets, software, sensors, automobiles, and household appliances to networking systems to transfer data without the need for human or computer intervention. The difficulty with the current method is that electronic voting machines lack any contemporary security mechanisms that allow voters to authenticate their identities before casting a vote, allowing for multiple duplicate or fake votes to be cast. To improve the security procedures, the suggested system is implemented utilizing RFID and IoT (Internet of Things). Instead of a voter id, an active RFID tag is utilized, which the system scans and compares to the fingerprints stored in the Aadhar database. The voter must scan the RFID tag to verify their identify, and then validate their identity using their fingerprints. This voting machine incorporates agile reading equipment (reader) for taking readings from RFID tags, as well as a finger print scanner for scanning finger prints. Individual people can efficiently cast their ballots if their prints match the database obtained; if it is not the case, then siren will sound to prevent the casting of counterfeit voters.

Ahmed Shamil et.al[10] have proposed that the act of dynamically recognizing persons based on their distinct behavioral or biological traits is known as biometric recognition (BR). It is a non-transferable link between a person and his or her true identity that cannot be lost, transmitted, or duplicated. Because of the rapid advancement of security systems, genetic trait-based identification is becoming increasingly crucial. The basic goal of the multimodal BR system is to make judgments by identifying persons according to their physiological characteristics. However, because to the high dimension of unimodal data in the temporal domain, these BR systems have difficulty making these judgments. This paper provides a decision fusion strategy for combining iris and fingerprint biometric in a procedure that does not require any preparation; this approach is based on a survey of the current work in this field. To excerpt features from fingerprint and iris biometric, the Gray-Level Co-occurrence Matrix (GLCM) with KNN is employed, with the AND gate used to determine the final decision. According to the data, the proposed fusion strategy outperformed single-modality alternatives significantly.The proposed method obtained a 95 percent efficiency level in terms of creating effective decisions for 20 test users.

Simon, et.al[11] proposed a new solution in decentralized network architectures in medical systems, including access points and multiple data nodes without a central point,to solve a number of vulnerabilities, including biometric leakage, which poses major threats as a result of the usage of stolen FV templates, and various spoofing and brute-force attacks in decentralized network architectures in health care systems, without a central point, incorporating access points and many data nodes. This paper adds to the body of knowledge by giving a complete analysis of reasonable alternatives and areas for further research, allowing researchers and engineers to continue developing FV biometric identification medical systems. There are also insights into the significance of such a technology and its incorporation into many medical applications and areas.

A.H. et.al[12] discussed that Finger vein recognition systems must address the issue of biometric data storage and processing while maintaining privacy. To validate the finger veins, modern biometric processes were applied. On the other hand, these methods are not specifically designed for finger vein patterns and therefore have the disadvantage of being sub optimal in many ways. They suggested an anti-alignment design protection technique that depends on an optimal binary sequence of the finger vein pattern while also employing Index of Maximum (IoM) hashing to meet the necessary privacy and security criteria The suggested technique has significantly lower computing costs as a result of a significantly decreased number of template comparisons performed for two templates. The suggested technique provides a promising balance between recognition performance loss and unlink ability.

Ying et.al[13] have proposed that fingerprint revocation is a concern. It is presented a new biometric templates based on local-similar image (LSIT). The LSIT's generation is divided into two parts: replacing and concealing the initial minutiae through expansion. This allows for the creation of reversible fingerprint templates with colored properties generated from fine details. The results show that the LSIT has impressive outcomes, indicating that it may be used to preserve and apply fingerprints in novel ways.

Simon et al[14]have discussed that With the purpose of safeguarding templates, they evaluated block-based warping sample modification techniques. The findings are weighed against the evolution of face recognition technology, which includes everything from "classic" hand-crafted characteristics to cutting edge deep-learning (DL)-based schemes. It turns out that face recognition technology can handle geometrical distortions induced by warping, as well as other sorts of variability such as location, lighting and expressive deformation thanks to high resistance.

Lee et.al[15] have proposed that the initial thumbprint template is regarded safe even if the transform and changed templates that employ that transform are compromised under the "Creating an Undoable Thumbprint Template" section of their paper. However, as this article indicates, this is not always the situation. If an attacker receives two changed blueprints from the very same fingerprint template and their modification settings, they can use a dictionary attack to reconstruct the original fingerprint template. They demonstrated that if two changed templates from the same fingerprint are corrupted, the surface folding transformation in "Generating Cancelable Fingerprint Templates" is unsafe. This means that the transformation employed in "Generating Cancelable Fingerprint Templates" is really not entirely non-invertible. As a result, a novel strategy is required to properly conceal the original biometric data even when several altered templates are exposed

## III. PROPOSED METHOD

This paper proposes a unique cancelable biometric system idea The framework is divided into five phases:

- Data capture
- Image Enhancement
- Minutiae Detection and Core Detection Algorithm
- Cartesian Block Transformation
- Reed-Solomon Error Correction
- Matching

### *A. Data Capture*

In this paper, the candidate's fingerprint will be captured using a 3M fingerprint scanning device. The fingers should be appropriately placed on the platen in order to catch. There should be no unnecessary illumination on the platen. Use the indications on fingerprint devices to put your fingers. On the gadget, the fingers should be put in the correct direction as well as clean the platen of the finger print device with a lint-free cloth on a regular basis to ensure optimal finger print capture. Then check devices for scratches, out-of-focus photos, and only partial photographs being taken on a regular basis. Excessively dry

or moist fingertips should be avoided as well as use of a damp cloth or a dry cloth to moisten the finger should be avoided as well.

*B. Image Enhancement*

The purpose of this step of the investigation is to mitigate for scratches and disruptions by generating a binary fingerprint image and accurately establishing its structure. The Gabor filter technique is utilized, which screens each pixel based on the frequency and direction of the ridge. Binarization, which employs a cutoff variable, and weakening, which decreases the ridge line width to one pixel, follow the enhancement phase.

*C. Minutiae Detection and Core Detection Algorithm*

In this article, we employ the minutiae identification algorithmic program[16], which traverses the enhanced picture to determine whether or not a component is a minutiae by inspecting its surrounding 8-neighboring pixels. If the component is on a ridge and has one neighboring ridge component then the component represents a ridge ending style of minutiae, on the opposite hand, if the component is on a ridge and has three neighboring ridge component then the component represents a bifurcation style of minutiae. The core points' location and orientation are then needed in order to accurately position the minutiae points with regard to these reference points. The cores of a fingerprint are represented by unique pixels called core points.Loops, deltas, and whorls are key points. We employ Kawagoe et al. fingerprint 's core identification technique [17], which separates the picture into small-regions, scans for direction patterns, and determines core points along a closed curve. It adds the difference between successive neighboring ridge direction angles for a pixel with its 8-neighborhood (x, y). With a tiny low threshold, the calculation's findings were supported:

•If the outcome is 0, (x, y) isn't a primary purpose.
•If the outcome is $2\pi$, (x, y) reflects a whorl type core .
•If the outcome is $\pi$, (x, y) represents a loop of some sort.
•If the outcome is $-\pi$, (x, y) reflects a delta type core.

Fig. 1. Captured Fingerprint

Fig. 2. Enhanced_thinned

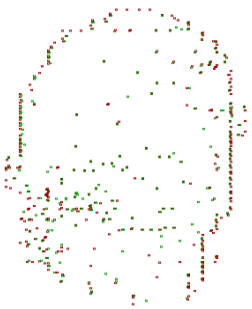

Fig.3.Enhanced_thinned_minutiaes

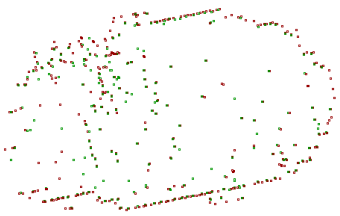

Fig.4.Enhanced_thinned_minutiaes_aligned

*D. Cartesian Block Transformation*

To cancel the fingerprint system, we apply Cartesian transformation in a unidirectional, irreversible procedure to recreate the minutiae points. We keep the revised fingerprint picture together with the transformation parameters rather than the original fingerprint image. The second organization on which the tiny points are drawn is divided into normal-sized blocks in Cartesian block transformation. The minutiae points are first put within the blocks that hold up their region, with closer minutiae points placed within the same or nearby blocks. Later, the transformation is carried out by rearranging the blocks with a matrix operation, and composition minutiae points are utilized to support the new block placements. The 2D coordinate system is broken into blocks of HxW dimension in our approach. Initial Cartesian blocks are numbered from one to |HxW| that is represented by a matrix C of size 1x|HxW|, and a metamorphosis matrix M of size |HxW|x|HxW| is every which way generated having values of either zero or one. As an example, if H and W both equal to 2, then C equals [1, 2, 3, 4]. The matrix multiplication with the M matrix that is formed is as follows:

$$C' = \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix} \begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} = \begin{pmatrix}3 & 2 & 4 & 3\end{pmatrix}$$

Fig.5. Cartesian Block Transformation

This means that the minutiae points in cartesian block 1 have been re-plotted to 3 and the minutiae points in cartesian block 2 have been re-plotted to 2. In the modified space, minutiae points in cartesian block 3 are mapped to 4, and 4 is mapped to 3, as seen in figure 5. Many cartesian blocks can also be routed to the very same cartesian block. Cartesian blocks are numbered according to their positions in a two-dimensional coordinate system. It's vital to notice that, throughout the registration stage, the first cartesian block for a specific minutiae purpose is not retained. Rather of maintaining the original positions of minuscule points, the transformation parameters are kept together with the modified locations. The transformation parameters include features such as the original fingerprint image's boundaries and the transformation matrix. However, when comparing for the candidate fingerprint model, the original cartesian blocks' minutiae points' remain intact to be used in the reed-solomon error elimination cryptographic recovery operation.

*E. Reed-Solomon Error Correction*

Reed-Solomon[18] is a technique for error correction. It generates parity data for a given input in such a way that it can duplicate the original input even if certain components are absent. Reed-solomon is used in several storage systems, including UNIX RAID and Yahoo's cold-storage. Reed-solomon divides the data into n equal parts and creates an input matrix, in which n is the size of the matrix. The software then creates a coding matrix of dimensions n + k, wherein k is the count of parity rows. First n rows of coding matrix has 1s within the diagonal and 0s for the remainder of the matrix cells.The coded knowledge is made by multiplying the coding matrix with the first matrix, due to the diagonal 1s within the coding matrix, The first n rows of coded data match the original message, whereas the last k rows are parity. As a consequence, every row in the coding matrix reflects to a row in the original data. As a result, each coding matrix row may correspond to a row of source data. If certain rows in the original message are missing, the corresponding rows in the coding matrix and the encoded matrix are erased, rendering the matrix multiplication equation acceptable on the left side with the original data. The inverse matrix of the latest coding matrix is then constructed and multiplied with each side of the latest equation. The original data matrix is formed on the left side of the equation. Figure 6 illustrates reed-solomon encoding of "ABCDEFGHIJKLMNOP" data input, as well as shows reed-solomon decoding when "IJKLMNOP" data is not present.The hashes of the minutiae points are used as input variables in our approach. Using the hashes of the minutiae points as data input, we employ the reed-solomon approach to execute reed-solomon on every one of the pre-transformed cartesian blocks. The original minutiae points of the original template are never exposed by employing hashes of the minutiae points, a method that protects the fingerprint owner's anonymity. For all of the pre-transformed rectangulars, we additionally execute a reed-solomon implementation, utilizing the hash of each cartesian block as input data. This method may be used to recover the lost minutiae point hashes for each cartisian block. As a result, we can calculate the whole hash of the biometric system, which we use in the matching process.

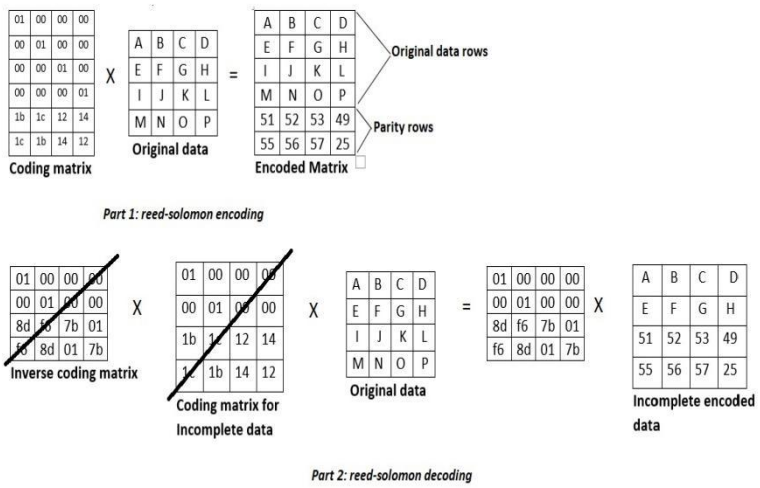


Fig.6. Example of Reed-Solomon Error Correction

*F. Matching*

During the matching phase, under go a series of processes to ensure that a candidate fingerprint picture does have the same total hashes as the original fingerprint image. The candidate fingerprint picture goes through the same pre - processing and modification processes as the original fingerprint picture, as described in sections A, B, and C. The cartesian transformation employs the same transformation variables (constraints and transformation matrix) as the enrollment of the original fingerprint picture. Furthermore, unlike the registration step, the candidate fingerprint picture retains its original cartesian block numbers. The matching technique compares the converted minutiae points of the contender fingerprint template to the transformed minutiae points of the original fingerprint template. Each one of the cartesian blocks was subjected to a separate comparison study. Geometrically close minutiae points in original as well as candidate fingerprint templates would indeed be converted to the very same cartesian block. As a result, the transformed candidate fingerprint template's minutiae points in cartesian block number x are only collated to the minutiae points in cartesian block number x of the altered original fingerprint template. The equality check for minutiae point types, and even the euclidean distance with an appropriate threshold, are used. If a match is found, the candidate fingerprint template's original cartesian block number is used to reverse the minutiae point conversion of the original fingerprint template. As a consequence, the completely matched minutiae points' original positions are restored. The cartesian blocks' recovered minutiae points are sent into the reed-solomon decoding procedure, which is detailed in section E, and a hash is produced as a result. The fingerprint pictures match if the produced hash matches the hash created during the registration process.

## IV. Result

In this work,we capture the finger print of the candidate which then gets stored in the database.Then the image is enhanced and then we apply minutiae detection algorithm and core detection algorithm to find the type of minutiae and core. After this we use cartesian transformation which transforms the minutiae points to make the fingerprint system cancelable. Matrix multiplication is used to rearrange the blocks and perform the transformation. The hash values of the minutiae points are then obtained using the Reed-Solomon error correcting algorithm. Following that, we utilize a matching technique to compare the converted minutiae points of the candidate fingerprint template to the transformed minutiae points of the original fingerprint template.

```
 1 /Users/keshavsarraf/.conda/envs/cancelable-
   fingerprint/bin/python /Users/keshavsarraf/dev/
   cancelable-fingerprint/fvs2.py
 2 Original:  images/sap.bmp
 3 Candidate:  images/sap2.bmp
 4 [2, 20, 7, 13, 25, 25, 1, 6, 5, 12, 2, 3, 24, 9, 5
   , 16, 3, 2, 13, 3, 24, 16, 14, 15, 22]
 5 [2, 20, 7, 13, 25, 25, 1, 6, 5, 12, 2, 3, 24, 9, 5
   , 16, 3, 2, 13, 3, 24, 16, 14, 15, 22]
 6 cartesian block:  1
 7 cartesian block:  2
 8 cartesian block:  3
 9 cartesian block:  4
10 cartesian block:  5
11 cartesian block:  6
12 cartesian block:  7
13 cartesian block:  8
14 cartesian block:  9
15 cartesian block:  10
16 cartesian block:  11
17 cartesian block:  12
18 cartesian block:  13
19 cartesian block:  14
20 cartesian block:  15
21 cartesian block:  16
22 cartesian block:  17
23 cartesian block:  18
24 cartesian block:  19
25 cartesian block:  20
26 cartesian block:  21
27 cartesian block:  22
28 cartesian block:  23
29 cartesian block:  24
30 cartesian block:  25
31 generated-hash:  Iz0oXRFHZ+VdidO8z4OUrg==
32 original-hash:  DmYBqacZYhUscPJb4adsbA==
33 generated and original minutias are NOT equal
34 trying reed solomon error correction codes
35 Avg-sim:  0.8
36 to-be-decoded:  ['HolCyLBI', 'Rm5mjdBB', '/ITTVsbb
   ', 'X7uA2qlV', 'eTpRI9Ml', 't0XdDGb5', 'CRUl2+My
   ', 'xxxxxxxx', 'qEayo4Wu', 'T6Ebvjkz', 'xxxxxxxx
   ', '9JpZJJyw', 'xxxxxxxx', 'Y1VAdl75', 'xxxxxxxx']
37 corrections:  [7, 10, 12, 14]
```

Fig. 7. Output Screen1

```
101 Avg-sim:  0.211904761905
102 to-be-decoded:  ['xxxxxxxx', 'xxxxxxxx', 'xxxxxxxx
    ', 'xxxxxxxx', 'xxxxxxxx', 'xxxxxxxx', 'xxxxxxxx
    ', 'xxxxxxxx', 'xxxxxxxx', 'xxxxxxxx', 'xxxxxxxx
    ', 'xxxxxxxx', 'xxxxxxxx', 'xxxxxxxx', 'KWD38FPE
    ', '1mdBlL1O', 'whEqIpDM', 'CgMP0nJB', 'd6X7f4Zd
    ', '6bT/lXiJ', 'yMhE0e4R', 'xxxxxxxx', 'xxxxxxxx
    ', 'mOAsBQyr', 'zzNpHu1g', 'xxxxxxxx', 'xxxxxxxx
    ', 'xxxxxxxx', 'xxxxxxxx', 'xxxxxxxx', 'xxxxxxxx
    ', 'xxxxxxxx', 'xxxxxxxx']
103 corrections:  [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
    11, 12, 13, 21, 22, 25, 26, 27, 28, 29, 30, 31, 32
    ]
104 decoded  ('qE+W4COJ', 'sqmnnYAy', 'hq07WOM+', '
    goWStRyp', 'EbjXkC8Q', 'DkZvnpzC', 'hgjkKbw8', '
    y4rO9PbI', 'dzwdyWWw', 'vuX1GqDC', 'xsusAA39', '
    Dc1CsyET', 'lFSUhJ+G', 'LKe/M7XM', 'KWD38FPE', '
    1mdBlL1O', 'whEqIpDM', 'CgMP0nJB', 'd6X7f4Zd', '
    6bT/lXiJ', 'yMhE0e4R', 'NF4vccAD', 'QhDKwgfG', '
    mOAsBQyr', 'zzNpHu1g', '/khxlyht', '+sL0fmqI', '
    F8eNFpwY', 'hA/JI9Qi', 'rrBXRzj4', '39+MihdW', '
    xDif6RUJ', 'jPxhrXi0')
105 c hashes are equal
106
107 generated-hash:  P1NU7Rf9j8YvVh/63gl/9g==
108 original-hash:  P1NU7Rf9j8YvVh/63gl/9g==
109 c generated and original minutias are equal
110
111 generated-hash:  xrD0PmYOo+XWLykBr5MkVQ==
112 original-hash:  6idsWO3U56JWqlKAaFOohg==
113 generated and original minutias are NOT equal
114 trying reed solomon error correction codes
115 Avg-sim:  0.291904761905
116 to-be-decoded:  ['tf287en3', 'xxxxxxxx', 'DzgAd3gl
    ', 'bDg0a3c6', '7wvOKDhf', 'DpED5W4s', 'O+QZX8Y4
    ', 'KeUBIPh3', 's9dZ42eE', 'N7hfVlhq', 'xxxxxxxx
    ', 'FjZiBtTa', 'iqgfE4p/', 'vudCmBLs', 'ftTaJ7TU
    ', '0zvyMYFD']
117 corrections:  [1, 10]
118 decoded  ('tf287en3', 'TRRN5xLd', 'DzgAd3gl', '
    bDg0a3c6', '7wvOKDhf', 'DpED5W4s', 'O+QZX8Y4', '
    KeUBIPh3', 's9dZ42eE', 'N7hfVlhq', '9gnZ9rpH', '
    FjZiBtTa', 'iqgfE4p/', 'vudCmBLs', 'ftTaJ7TU', '
    0zvyMYFD')
```

Fig. 8. Output Screen2

```
845 num-cart:  22.0 num-cart-match:  1.0
846 processed:  (2, 1) (1, 2)
847 --next-pair--
848
849 True Positives:
850 ('images/sap.bmp', 'images/sap2.bmp')
851 ('images/sap2.bmp', 'images/sap.bmp')
852 False Positives:
853 True Negatives:
854 ('images/sap.bmp', 'images/101_1.tif')
855 ('images/sap2.bmp', 'images/101_1.tif')
856 ('images/101_1.tif', 'images/sap.bmp')
```

Fig. 9. Output Screen3

```
857 ('images/101_1.tif', 'images/sap2.bmp')
858 False Negatives:
859
860 Num-try:  6     Num errors:  0 xmatchthreshold:
    12.0    ymatchthreshold:  12.0 rmdivide:  4 4
861 Precision:  1.0     Recall:  1.0    Fmeasure:  1.0

862
863 avg_avg_sim:  0.265341537077
864
865 Process finished with exit code 0
866
```

Fig. 10. Output Screen4

## V. Conclusion And Future Work

While biometric authentication seems to provide huge benefits over passcode and token-based security, it also poses security and privacy concerns that must be addressed. To solve this difficulty, we presented many breakthroughs that came from both the cryptography and biometric communities. The benefits of cancelable biometric over many other ways were explored, as well as a scientific investigation of how this methodology was utilized to create a fingerprint database. Several cancelable algorithms were investigated, together with Cartesian and Reed Solomon. We may deduce from the data that a cancelable transformation can be utilized for the characteristic domain without producing considerable performance reduction.

## References


1. Wang, Song, and Jiankun Hu. "A Hadamard transform-based method for the design of cancellable fingerprint templates." 2013 6th International Congress on Image and Signal Processing (CISP). Vol. 3. IEEE, 2013.
2. Ratha, Nalini K., et al. "Generating cancelable fingerprint templates." IEEE Transactions on pattern analysis and machine intelligence 29.4 (2007): 561-572
3. Kaur, Harkeerat, and Pritee Khanna. "Random distance method for generating unimodal and multimodal cancelable biometric features." IEEE Transactions on Information Forensics and Security 14.3 (2018): 709-719.
4. Hammad, Mohamed, Yashu Liu, and Kuanquan Wang. "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint." IEEE Access 7 (2018): 26527-26542.
5. Kim, Jihyeon, and Andrew Beng Jin Teoh. "One-factor cancellable biometrics based on indexing-first-order hashing for fingerprint authentication." 2019 24th International Conference on Pattern Recognition (ICPR). IEEE, 2019.
6. Dong, Xingbo, Zhe Jin, and Andrew Teoh Beng Jin. "A genetic algorithm enabled similarity-based attack on cancellable biometrics." 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2019.
7. Lee, Ming Jie, et al. "A Tokenless Cancellable Scheme for Multimodal Biometric Systems." 2021 IEEE 10th International Conference on Computers & Security (2021): 102350.
8. Sudhakar, Tanuja, and Marina Gavrilova. "Cancelable biometrics using deep learning as a cloud service." IEEE Access 8 (2020): 112932-112943.
9. Mansingh, PM Benson, T. Joby Titus, and VS Sanjana Devi. "A secured biometric voting system using RFID linked with the Aadhar database." 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2020.
10. Mustafa, Ahmed Shamil, Aymen Jalil Abdulelah, and Abdullah Khalid Ahmed. "Multimodal biometric system iris and fingerprint recognition based on fusion technique." 2019 24th International Conference on Pattern Recognition (ICPR). IEEE, 2019.
11. Kirchgasser, Simon, et al. "Template protection on multiple facial biometrics in the signal domain under visible and near-infrared light." 2020 8th International Workshop on Biometrics and Forensics (IWBF). IEEE, 2020.
12. Mohsin, A. H., et al. "Finger vein biometrics: taxonomy analysis, open challenges, future directions, and recommended solution for decentralised network architectures." Ieee Access 8 (2020): 9821-9845.
13. Li, Zhaozheng, Ying Bao, and Theyimin Lei. "Generating Cancellable Fingerprint Template Using Local-Similar Image." 2020 IEEE 3rd International Conference on Electronics and Communication Engineering (ICECE). IEEE, 2020.
14. Kirchgasser, Simon, et al. "Is warping-based cancellable biometrics (still) sensible for face recognition?." 2020 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2020.

15. Shin, S.W., Lee, M.K., Moon, D. and Moon, K., 2020. Dictionary attack on functional transform-based cancelable fingerprint templates.
16. Hong, L., Wan, Y., and Jain, A. (1998). Fingerprint image enhancement: algorithm and performance evaluation. IEEE transactions on pattern analysis and machine intelligence, 20(8):777–789.
17. Kawagoe, M. and Tojo, A. (1984). Fingerprint pattern classification. Pattern recognition, 17(3):295–303
18. Reed, I. S. and Solomon, G. (1960). Polynomial codes over certain finite fields. Journal of the society for industrial and applied mathematics, 8(2):300–304.

**IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.**