Abstract—This paper proposes a robust authentication mechanism based on semantic segmentation, encryption and data hiding. In user authentication schemes involves smart cards using dynamic users’ identities per transaction section. These methods aimed to overcome a common drawback of older remote authentication schemes using smart cards: user’s identity was static in all the transaction sessions, which may leak some information about that user and can create risk. So this problem can be solve by using Biometric device so the scheme overcomes the wireless channels under loss tolerant transmission protocols, we aims to ensure: (a) robustness against deciphering, noise and compression, (b) good encryption capacity, (c) ease of implementation. For this purpose we: (a) employ wavelet based steganography, (b) biencryt biometric signals to allow for natural authentication, (c) the encrypted biometric signal is hidden in the VO, which can be detected in modern applications that involve teleconferencing. Even though biometric keys are strong technique for data encryption by using Blowfish, because they are stored in the database, there remains a chance for the keys to be eavesdropped by unauthenticated users which makes the system vulnerable.

I. INTRODUCTION

Person authentication is one of the most important issues in contemporary societies. It ensures that a system’s resources are not obtained fraudulently by illegal users. Real-life physical transactions are generally accomplished using paper ID while electronic transactions are based on password authentication, the most simple and convenient authentication mechanism over insecure networks. In [1], a remote password authentication scheme was proposed by employing a one-way hash function, which was later used for designing the famous S/KEY one-time password system [2]. However, in such schemes, a verification table should be maintained on the remote server in order to validate the legitimacy of the requesting users; if intruders break into the server, they can modify the verification table. Therefore, many password authentication schemes [3–4] have recognized this problem, and different solutions have been proposed to avoid verification tables.

One very popular solution is based on cryptographic keys, which are long and random (e.g., 128 bits for the Advanced Encryption Standard [8]), thus it is difficult to memorize. As a result, these keys are stored somewhere (e.g., on a server or smart card) and they are released based on some alternative authentication mechanism (e.g., password). However, several passwords are simple and they can be easily guessed (especially based on social engineering methods) or broken by simple dictionary attacks [9]. In this case, user protection is only as secure as the password (weakest link) used to release the correct decrypting key for establishing user authenticity. Simple passwords are easy to guess; complex passwords are difficult to remember, and some users tend to “store” complex passwords at easily accessible locations. Furthermore, most people use the same password across different applications; if a malicious user determines a single password, they can access multiple applications.

Many of these password-based authentication problems can be confronted by the incorporation of biometrics [5, 6]. Biometrics authentication refers to establishing identity based on the physical and/or behavioral characteristics of a person such as face, fingerprint, hand geometry, iris, voice, way of walking, and so forth. Biometric systems offer several advantages over traditional password-based schemes. They are inherently more reliable, since biometric traits cannot be lost or forgotten, they are more difficult to forge, copy, share, and distribute, and they require the person being authenticated to be present at the time and point of authentication. Thus, a biometrics-based authentication scheme is a powerful alternative to traditional systems, and it can be easily combined with password techniques to enhance the offered security.

In order to further promote the wide spread utilization of biometric techniques to applications over error prone networks, increased security and especially robustness of the biometric data is necessary. Towards this direction, proper combination of encryption and steganography can achieve this goal. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood. In a real-world scenario, encryption can be applied to the biometric signals for increasing security; the templates that can reside in either a central database or a token (e.g., smart card, or a biometric-enabled device such as a cellular phone with a fingerprint sensor), can be encrypted after enrollment. During authentication, these encrypted templates can be decrypted and used for
generating the matching result with the biometric data obtained online.

As a result, the encrypted templates are secured since they cannot be utilized or modified without decrypting them with the correct key, which is typically secret. On the other hand, steganographic methods can hide encrypted biometric signals so that they cannot be seen, hence, reducing the chances of illegal modifications. Generally, steganography utilizes typical digital media such as text, images, audio, or video files as a carrier (called a host or cover signal) for hiding private information in such a way that unauthorized parties cannot detect or even notice its presence [7]. Several steganographic algorithms have been proposed in the literature, most of which are performed in pixel domain, where more capacity [8] is provided. Many of the existing approaches are based on least significant bit (LSB) insertion, where the LSBs of the cover file are directly changed with message bits. Examples of LSB schemes can be found in [6]. However, LSB methods are vulnerable to extraction [6, 7], and they are very sensitive to image manipulations. For example, converting an image from BMP to JPEG and then back would destroy the hidden information [6].

1.1 STEGANOGRAPHY

Steganography is the art and science of hiding communication, a steganographic system thus combines hidden content in unremarkable cover media so as not to attempt an eavesdropper’s attack. In the past, people used hidden tattoos or invisible ink to convey steganographic information content. Today, computer and network technologies provide easy-to-use communication channels for steganography. The information-hiding process in a steganographic system starts by identifying a cover medium’s redundant bits (those that can be modified without destroying that medium’s integrity). The embedding process creates an stego medium by replacing these redundant bits with information from the hidden message. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium’s statistical properties. The process of finding these distortions is called statistical steganalysis. The data security approach when combined with encryption and steganographic techniques for hidden communication by hiding it inside the multimedia files[4][5].

The maximum results are achieved by providing the security to information before transmitting it through the internet[2]. The files like audio, video, images, contains collection of bits that can be further translated into images, audio and video.

1.2 Contribution and plan of this paper

The main aim of this project is to reduce the amount of paperwork involved, widespread corruption; misuses of cards and duplications. To reduce the time complexity of the manual data entries and checks. Many fake ration card users exist which is against the law, it is used to avoid such things. Our system is used to protect the products of Fair Price Shop in Black markets. Finally the purchased details are sent as SMS to the customer mobile phones.

II. LITERATURE SURVEY

Several steganographic algorithms have been proposed in the literature, most of which are performed in pixel domain, where more capacity [9] is provided. Many of the existing approaches are based on least significant bit (LSB) insertion, where the LSBs of the cover file are directly changed with message bits. Examples of LSB schemes can be found in [10]. However, LSB methods are vulnerable to extraction [11], and they are very sensitive to image manipulations. For example, converting an image from BMP to JPEG and then back would destroy the hidden information [12]. The SSIS incorporated the use of error control codes to correct the large number of bit errors. In [14], the message is hidden in the sign/bit values of insignificant children of the detail sub bands, in non smooth regions of the image. Using this technique, steganographic messages can be sent in lossy environments, with some robustness against detection or attack. However, low losses are considered, and the problem of compression remains. A very interesting approach is proposed in [15]. The message is comprised of two components: a soft-authenticator watermark for authentication and tamper assessment of the given image, and a chrominance watermark employed to improve the efficiency of compression. The approach is implemented as a DCTDWT dual domain, but, unfortunately, the authenticator watermark is not encrypted, making it possible to extract it. There are also some schemes focusing on steganography of biometric signals. In [16], an amplitude modulation based steganographic scheme is proposed, which, however, is not tested under compression or lossy transmission. In [17], a wavelet-based steganographic method for minutiae embedding is proposed. Nevertheless, if opponents know the embedding algorithm, they can easily extract the hidden information. In [18], fingerprints are hidden in the region of interest of images. Both DFT and DWT domains are examined. However, again, no encryption is incorporated, thus it is easy to extract the hidden fingerprints. Another interesting, but not resistant to compression, method is proposed in [19], where a remote multimodal biometrics authentication framework that works on the basis of fragile watermarking is designed. Finally, in [20], a DCT-SVD based watermarking scheme is proposed for ownership protection using biometrics. The scheme is not tested under compression or lossy transmission. In order to confront
the problem of user authentication, in this paper, we propose an efficient wavelet-based steganographic method for biometric signals hiding in video objects, which focuses on optimizing the authentication rate of hidden biometric data over error prone transmissions. Interesting techniques for object-oriented data hiding have been presented in the literature, for example [18,19], however, most of them do not particularly consider the case of biometric data

In [21], Biometrics-based human verification over remote channels under flaw tolerant conventions. The proposed approach a few portable applications could advantage. For instance, in a rising situation, let us envision that a client might want to be confirmed through her mobile phone, tablet and so forth. Her versatile gadget has a camera, while its touch-screen works together with a fingerprints catching application. In the event that the sign quality is low, mistaken parcels might touch base at the collector. Along these lines as plan like the proposed in required.

Automatic extraction of semantically significant video objects for inserting the scrambled biometric data: The greater part of the current plans doesn’t consider semantically significant VOs as hosts, yet an entire picture. The proposed plan offers some conceivable points of interest. Firstly, the plan gives an auxiliary reciprocal confirmation instrument on the off chance that when the individual under confirmation is likewise caught by the camera. Along these lines her face and body is transmitted together with another biometric highlight for conceivable twofold validation. Besides, in each late exchange, the general structural engineering can store the most recent example pictures of one’s face and body [17]. This could help in cases of half breed remote validation, when both a machine and a human remotely validate a man. The machine can verify the unique mark and the human can confirm the face (like the teller does in a bank). Another point of preference needs to do with more proficient transmission capacity utilization, particularly in the previously stated instance of cross breed remote validation. A picture more often does not just contain semantically important data additionally foundation squares. Then again, keeping in mind the end goal to conceal a particular measure of data, a host with legitimate limit ought to be chosen. In the event that the host is a picture, at that point unessential pieces will likewise be transmitted, involving profitable data transmission. Despite what might be expected, when the host is a semantic VO, all transmitted data is significant to the validation errand. To wrap things up, the proposed plan takes into consideration more effective rate control and can better face activity clogs. For instance, in an average steganographic calculation which utilizes pictures, if activity clog happens, all picture obstructs (with the exception of those that contain shrouded data) would be presumable considered of equivalent significance. On the other hand, the proposed plan is content-mindful. If there should be an occurrence of activity blockage, the rate control instrument could dispose of obstructs from the body area that don’t likewise contain covered up data, rather than disposing of face territories.

In [22], works like a one-time cushion, to scramble biometric identifiers: Symmetric encryption is speedier, in this manner in contemporary frameworks a key of size $2n$ bits is created and it is traded between the conveying elements, utilizing open key cryptography. Be that as it may, despite the fact that extensive keys are thought to be sheltered, it has been demonstrated that any figure with the ideal mystery property must use keys with adequately the same prerequisites as one-time cushion keys. For our situation, biometric identifiers are scrambled by a disorderly figure, which works like a one-time cushion in wording of key size, subsequent to the produced key has size equivalent to the size of the information to be encoded. Tumultuous frameworks are useful for such sorts of errands, since they display an interminable number of insecure circles, consequently an interminable number of various qualities. Advancement of the turbulent figure relies on upon its starting conditions what's more, the encoded estimations of the biometric identifiers and in this manner just the beginning conditions ought to be traded between the conveying substances.

### III. EXISTING SYSTEM

Password-based remote user authentication schemes are widely investigated, with recent research increasingly combining a user’s biometrics with a password to design a remote user authentication scheme that enhances the level of the security. This paper we propose want to access different application servers. To solve an anonymous multi-server authenticating key agreement scheme based on trust computing using smart cards, password, and biometrics. The user only needs to register with the registration center once and then can access different application servers. The privacy of the user has attracted increasing attention from both industry and academia. Therefore, anonymous authentication involves verifying that a user does not use the real identity to execute the authentication procedure.

### Issues in Existing System

1. **Traceable problem:** In cryptography, the user’s privacy includes anonymity and untraceability, where anonymity means that an adversary cannot obtain the user’s real identity, and untraceability means that an adversary cannot acquire the user’s behavior trajectory.

2. **The distribution of PSK:** The distribution of the PSK is a trade-off issue. If the PSK is only kept in the RC, the server’s compromise problem will not happen.

### IV. PROPOSED SYSTEM

In proposed system firstly video conferencing the object is extracted with the host object then it is going through the hiding module this consist of QSWT I. e. Qualified Significant Wavelet Tree this is beneficial where lossy transmission and compression in wireless network. In this module the input signal is also encrypted with biometric samples so individuals identity is encrypted then vectorise this biometric signal [4]. Then stego object which is compressed is transmitted to decompress through
The proposed remote human confirmation plan over remote channels under misfortune tolerant transmission conventions plans to guarantee: (a) power against interpreting, clamor and pressure, (b) great encryption limit, and (c) simplicity of execution. For this reason we: (an) utilize wavelet based steganography, (b) encode biometric signs to take into cons iteration normal confirmation, (c) include a Chaotic Pseudo-Random Bit Generator (C-PRBG) to make the keys that trigger the entire encryption to build security, and (d) the scrambled biometric sign is covered up in a VO, which can dependably be recognized in present day applications that include video chatting. The general structural engineering and information stream of the proposed plan is shown in 1. At first the biometric sign is encoded by joining a turbulent pseudo-arbitrary piece generator what's more, a disarray driven figure, taking into account blended input what's more, time variation S-boxes (see likewise Fig. 2). The utilization of such an encryption system is defended subsequent to

1) Mayhem presents affectability to beginning conditions.
2) A C-PRBG factually works exceptionally well as a one-time cushion generator,
3) Usage of famous open key encryption systems, for example, RSA or El Gamal, can't give suitable encryption.

Encryption calculations consolidate symmetric and open key cryptography. Then again the security of these calculations depends, in principle, on the trouble of rapidly factorizing substantial numbers or settling the discrete logarithm issue, and, by and by, on the trouble of recording acoustic spreads from PCs amid operation. However both levels (hypothetical and down to earth) might be tested by late advances in number hypothesis, conveyed figuring and acoustic cryptanalysis.

A. Advantages of proposed system

1. It addresses both spatial and temporal domains, which leads to detecting various malicious changes in spatial and time domains.
2. It is faster and lower complexity compared to existing algorithms, making it practical and suitable for real-time applications
3. Hiding Capacity of the secret data bits is high.
4. Hiding capacity was based on the pixel number corresponding to the two highest peaks of the image histogram

4.1 SYSTEM MODEL

Every user has to registering their profile information into the server. Once registration process completed, server will storing all users face in their own database. A server capturing the face on video mode automatically. Captured user face can be store in server. Once human face capturing process is completed, server will capture the user appropriate biometrics. Here biometrics are not directly storing into the server. Every biometrics has to be encrypted and watermarked into the user face. So every watermarked image is maintained in the server. remote server authentication is going to be performed. If user wants to access the application means he/she has to give his face and biometrics to the server. Server will match face with every face on the database. If server identified the matched face means, server will extract the fingerprint from that image. After extracting, server checks the face and biometrics into the matched face and biometrics. It is represented in the figure 2. If both are matches only server will authenticate the user. Once all authentication process was completed, user can access the application. Here we are going to develop ration shop application. Now a day’s person want to buy ration products means they will use ration card and buy the product. In ration shop they are not validating that appropriate ration card holder only buy their own product. So for validating on ration shop, we are going to apply this authentication. For every time user has to purchase product means, he/she has to give his own face and biometrics into the server. Once validating only user can buy ration product. After purchasing the product user can pay amount through bank transaction.
Every biometrics has to be encrypted and watermarked into the user face. For encryption here we are going to apply blowfish algorithm. This algorithm read every pixels values of the biometrics and change the pixel values of it. After encryption process, server will embed encrypted biometrics into the human face. For embedding (watermarking) we are going to apply Least Significant Bit (LSB) techniques. These techniques will read every rows and columns of the biometrics and embedding into the appropriate rows and columns of the human face. So every watermarked image is maintained in the server.

Blowfish where the key does not change often, like communication link or an automatic file encryptor. Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms such AES, DES and 3 DES etc. Blowfish is a symmetric block encryption algorithm designed in consideration with

i. Fast : It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.

ii. Compact: It can run in less than 5K of memory.

iii. Simple: It uses addition, XOR, lookup table with 32-bit operands.

iv. Secure: The key length is variable, it can be in the range of 32~448 bits: default 128 bits key length.

V. IMPLEMENTATION

The proposed system of this project is divided into three major modules and described as below.

1. DATA ENCRYPTION
2. EMBEDDED SYSTEM
3. STEGO OBJECT COMPRESSION

5.1 MODULES DESCRIPTION

5.1.1 DATA ENCRYPTION

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

Generating the Sub keys

The sub keys are calculated using the Blowfish algorithm:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one
equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm. In total, 521 iterations are required to generate all required subkeys. Applications can store the subkeys rather than execute this derivation process multiple times.

5.1.2 EMBEDDED SYSTEM
After the converting our information in secret code or encrypted form we need to patch that data in the image. We use least significant bit for the patching of data because of following reason.

a. Because the intensity of image is only change by 1 or 0 after hiding the information.
b. Change in intensity is either 0 or 1 because the change at last bit
   e.g. 11111000 ⊕ 11111001

The change is only one bit so that the intensity of image is not effected too much and we can easily transfer the data.

Steps:
1. Initially image hiding process, convert cover color image into RGB file format, then extract the R(Red) component alone.
2. Then convert The Red component decimal number in to binary number
3. Convert the Secret binary image shares into binary numbers.
4. Take the first binary number of Secret Shares then convert one’s complement and replace in to 4th bit of the Each Red component binary bit of cover color image
5. By repeating this process until all the binary numbers of shares has to be completed
6. Extracting process is reversible of hiding process

5.1.3 STEGO OBJECT COMPRESSION
Huffman compression belongs into a family of algorithms with a variable code word length. That means that individual symbols (characters in a text file for instance) are replaced by bit sequences that have a distinct length. So symbols that occur a lot in a file are given a short sequence while other that are used seldom get a longer bit sequence. A practical example will show you the principle: Suppose you want to compress the following piece of data: ACDABA Since these are 6 characters, this text is 6 bytes or 48 bits long. With Huffman encoding, the file is searched for the most frequently appearing symbols (in this case the character „A’ occurs 3 times) and then a tree is build that replaces the symbols by shorter bit sequences. In this particular case, the algorithm would use the following substitution table: A=0, B=10, C=110, D=111. If these code words are used to compress the file, the compressed data look like this: 01101110100 It means that 11 bits are used instead of 48, a compression ratio of 4 to 1 for this particular file. Huffman encoding can be further optimized in two different ways: i. Adaptive Huffman code dynamically changes the code words according to the change of probabilities of the symbols. ii. Extended Huffman compression can encode groups of symbols rather than single symbols.

Every user has to registering their profile information into the server. Once registration process completed, server capturing the face. And automatically storing into the server. Each stored image file as one text file to read it. Once human face capturing process is completed, server will capture the user appropriate biometrics. Here biometrics are not directly storing into the server each stored image file as one text file to read it. Every biometrics has to be encrypted and watermarked into the face. Admin will display all registered user in the application and it will be update the stock details daily and stored in database. User can only purchase updated stock in the application. For watermarking we are going to apply Least Significant Bit (LSB) techniques. These techniques will append byte file of every rows and columns of the biometrics into the appropriate rows and columns of the human face to read binary value and then the image get embedded. For compression we are going to apply Huffman compression techniques. These techniques will measure the hidden image file size and it compress image for reducing size of image store in server. Finally the process are done successfully The compressed image file are transmitted to server. The server will have all encrypted file, data hiding and compression image separately. In this phase we register the user information and stored safely in server by using several technique and In admin side we update the stock details then it apply some process to maintain security and avoid duplicate. It is represented in the following figures.
VI. CONCLUSION

Biometric signals enter more and more into our everyday lives, since governments, as well as other organizations, resort to their use in accomplishing crucial procedures (e.g. citizen authentication). Thus there is an urgent need to further develop and integrate biometric authentication techniques into practical applications. Towards this direction in this paper the domain of biometrics authentication over error-prone networks has been examined. Since steganography by itself does not ensure secrecy, it was combined with a blowfish encryption system. In future research, the impacts of pressure and portable transmission of other shrouded biometric signals (e.g. voice or iris) ought to additionally be inspected.

REFERENCE


