International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 11 | Nov 2020 www.irjet.net p-ISSN: 2395-0072

Multimodal Biometric Authentication System using Steganography

Naziha Mohammed Al-Aidroos[1], Hesham Awadh Bahamish[2], Mohammed Abdullah Bamatraf[3]

[1,2,3]*Assistant Professor, Computer Science Department, Computers & Information Technology Faculty, Hadhramout University, Yemen*

Abstract - *With the rapid development and increasing growth in the ways of transmitting data across networks, especially after the Corona pandemic, where most financial or commercial transactions have taken place via the Internet, this has become an urgent case for developing new reliable user authentication methods. In this paper, we suggesting to use a new biometric authentication system to provide an electronic ID as a combination of biometrics measures (e.g. Face and Fingerprint authentication), hash functions and steganography technique. Biometric authentication is a process where the biometric data of a person is used to verify his identity. In the proposed scheme, the person's fingerprint is hashed and hidden in his face image in such a way that the features, which are used in face matching, are not significantly altered during hiding process. This provide an efficient secure multimodal biometric authentication system.*

Key Words: Steganography, Data Hidden, Data Security, Biometric, Authentication, Face, Fingerprint, Hash Function.

1. INTRODUCTION

In recent community, the ability to confirm individual's identities in real time is a main requirement in many systems such as manage bank accounts, electronic commerce, data transfer, etc. As people become more and more mobile in a highly networked world, the process of accurately identifying individuals becomes even more critical as well as challenging. Failure to identify individuals correctly can have grave repercussions in community ranging from terrorist attacks to identity fraud where a person loses access to his own bank accounts and other personal information.

Indeed, the last two decades have seen an increasing growth of using biometrics systems. Without a doubt, biometric technology is already creating a significant impact on our society, this impact dramatically increased at the recent time because the occurrence of a corona pandemic (COVID-19), which would create such widespread disruptions of work and personal lives. COVID-19 has created not only disruption but also an acceleration of digital transformation across many aspects of our lives. The use of online and mobile transactions and communications has taken a huge leap forward during the pandemic, creating new opportunities and new threats. All of these reasons caused the needing to develop a new authentication systems.

In online systems, one of the traditional authentication methods is by using a simple username and a password. Although an interesting methods to identify users are appear daily, the password based authentication still as one of the most preferred methods of all, because its ease of getting memorized at no cost and users' ability to use them in their daily life.

As time changes, various authentication methods have been introduced, some in biological, while others in graphical passwords. Along with the use of passwords, these methods provide an even higher level of security for user logins. [1]

In this paper, we propose an effective and adequate multimodal biometric authentication system using a combination of a face and fingerprint biometrics, hash function and the steganography technique. The user fingerprint features are hashed using a hash function such as MD5 algorithm, this value is hidden inside the user face image as a cover image using steganography technique like LSB. This multimodal biometric authentication can help the system in increasing the security and adequacy in compare to unimodal biometric authentication, and it would be very hard for an attacker to fraud the system because of two distinct biometrics features and one of them are hashed.

The rest of the paper is organized as follows. The theoretical background is presented in Section 2. In Section 3 , the proposed scheme is elaborated, followed by the security discussion in Section 4. Conclusions presented in Section 5.

2. BACKGROUND

2.1 Steganography

Steganography is the art and science of concealing a secret data inside a cover object in a way that its existence is completely hidden, so the intended attacker cannot be able to detect the data existence.

In steganography, the cover object can be any media file such as image, text, audio, and video. Once a secret message is embedded in a cover object, the stego-object is produced. Image steganography is one of the common widely steganographic techniques.

An image steganography technique aims at three core principles:

1- **Capacity**: the amount of data that can be hidden in the cover image.

2- **Imperceptibility**: the visual quality of the stego-image after embedding process.

3- **Robustness**: refer to amount of modification the stego object can resist before an attacker can modify or destroy the hidden information.

Several an image steganographic methods have been developed. The Least-Significant-Bit (LSB) data hiding method is one of the earliest methods, it is simple to understand, easy to implement, and it produces an image that almost similar to a cover image called stego-image.

2.1.1 Classical LSB Method

An image is represented in a computer as array of integers called pixels (light intensities points). Digital images are typically stored in either 24-bit (color images) or 8-bit (grey images) per pixel.

In LSB method, the hidden is done by replacement the LSB's of cover images with a secret data. This replacement process should not effect on a cover image, therefore, the unauthorized user will not be able to notice the hidden data.

As an example of LSB method, suppose we want to hide the secret data '10000001' in a cover image as follows:

Cover Image:

00100011 11101101 11001110 00100111 11001000 11101001 11001010 00100111

Secret Message: 10000001

Stego Image:

00100011 11101100 11001110 00100110 11001000 11101000 11001010 00100111

Where the bold bits represent the changed bits.

We also can replace more than one bit with preserving the image quality without any noticeable changing.

2.2 Authentication

Authentication is a process of verifying a user's legitimate right before secure resources can be released. [2]

The authentications is divided into two main categories: traditional and biometric. Figure 1 presented a summary of these categories. [3]

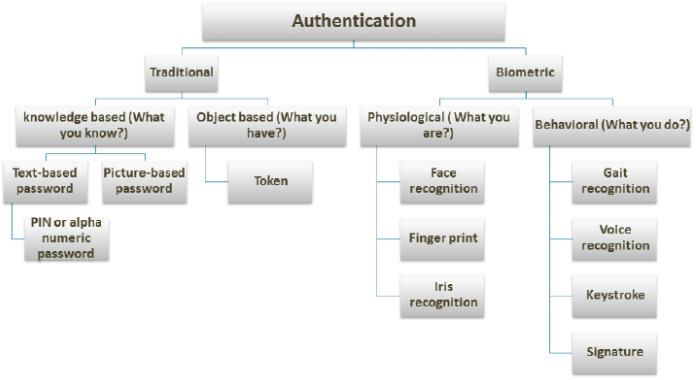

Fig -1: Classification of authentication techniques

2.2.1 Biometric Authentication

Biometric authentication is the science of establishing the identity of a user, towards a system, based on his/her physical or behavioral attributes. The biometric authentication domain has obtained an increasing publicity during the last decade. It divides into two major categories: [5]

(a) **Physiological**, which uses certain physical identifying attributes.
(b) **Behavioral**, which uses certain identifying attributes from an individual's movement or the manner in which they interact with peripheral devices.

Various examples of both biometrics categories are shown in Figure 1.

2.2.1.1 Components of a Typical Biometric System

A typical biometric authentication system consists of five modules as shown in Figure 2. [3]

- **Sensor module**: is used to capture user's raw biometric data. An example is camera used to take a picture of human face.
- **Feature extraction module**: is used to process the acquired biometric data to extract a set of features. For example, features on the surface of a face, such as the contour of the eye sockets, nose, and chin.
- **Matcher module**: is used to compute matching scores of comparing the extracted features against the stored ones.
- **System database module**: is used to store the biometrics templates of features the enrolled users [6].
- **Decision-making module**: is used to either determine the user's identity or confirm the users claimed identity [7].

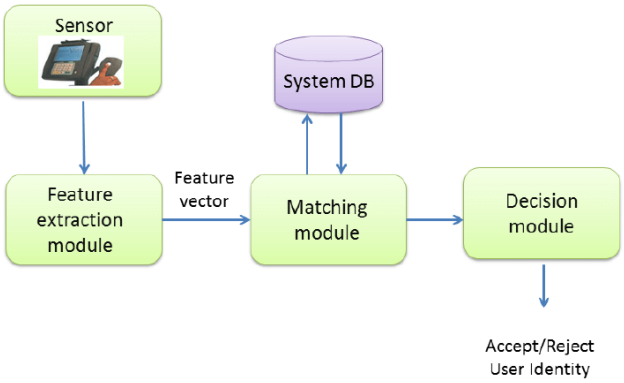

Fig -2: Biometric modules

In the proposed scheme, we used a combination of fingerprint and face recognition biometrics, the following sections explain these types of biometrics.

2.2.1.2 Fingerprint authentication

Fingerprint biometric is one of the most common widely biometric authentication techniques today. Where it is known that no fingers have similar prints, even from the same individual or identical twins. Traditional finger scanning technique is analysis of small unique marks of the finger image known as minutiae (finger image ridge endings, bifurcations or branches made by ridges). [8]

Fingerprint authentication include two phases: enrolment and verification [8, 9, 10]:

- **Enrolment phase**, a fingerprint image is obtained from a sensor, and then extracting the unique features by process it. These features are used to form a fingerprint template, finally stored this template in a secure database.
- **Verification stage**, the same process is followed to extract fingerprint query features. A matching process is implemented by comparing the query features with the stored template and calculating a similarity score. If the score is higher than a pre-defined threshold, then the query fingerprint is considered to match the template, and the authentication result is 'success'. Otherwise, the authentication fails. A fingerprint authentication process is described in Figure 3.

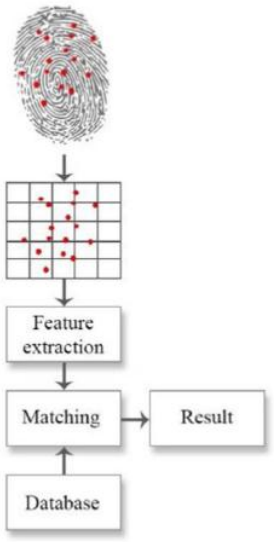

Fig -3: Fingerprint authentication

2.2.1.3 Face authentication

Face authentication can be done manually to compare a photograph on an identity card with the face of the bearer of that card. In addition, the human face can be represented digitally in the form of eigenfaces. Eigenfaces are constructed by performing principal component analysis (PCA) on a large set of facial imagery and are represented as a set of eigenvectors. They are, in effect, the sum of chosen components from a collection of standardized facial ingredients that best represent a subject's face [5, 11].

As fingerprint authentication, a face authentication follows a similar phases of enrolment and verification (see Figure 4).

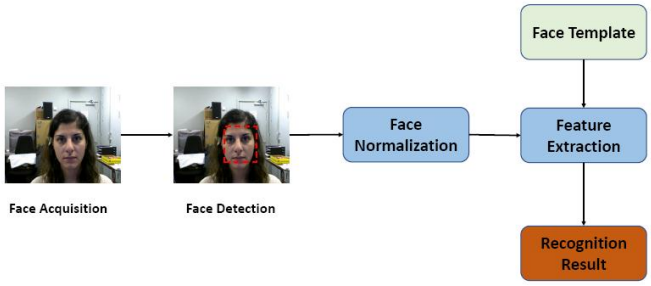

Fig -4: A face authentication [12]

2.2.1.4 Biometric Authentication Systems Security

Majority of current authentication and verification systems are dependent on the 'something you know or have' philosophy. The users required to remember multiple passwords or to possess tokens. However, these passwords can be easily forgotten or can become exposed if they are written down. Tokens can be lost, this will make the users cannot be able to access to the needed services or systems. An individual's biometric attributes can uniquely identify a person using their personal attributes so that there is no need to remember passwords or carry a token, because

these biometric attributes do not need to be remembered and can rarely be lost (only, for example, through severe injury to fingers or eyes). While biometric authentication and verification systems are adequate to use, it does make the security of the digitized biometric data a serious matter. If the attacker can access to this data, he can use it to conduct attacks by different ways. [5]

2.3 Hash function

A hash function *H* is a mathematical function transforms the input *m* (variable length) to a hash value *h* (fixed length); *h* =*H*(*m*). Hash function *H* is said to be a one-way function if it is hard to invert [13], that is, given a hash value *h*, it is computationally infeasible to find some input *x* such that *H*(*x*)= *h*.

In the proposed scheme the user fingerprint features are used as input to the hash function to produce a hash value which embedded later inside the user face image (cover image), this step is provided to maintain fingerprint data integrity. In case the biometric data is hashed, even a small alteration in it can lead to completely different hash value. This will cause non-matching between altered data and stored one. Therefore, the hash-based system must adhere to the following additional properties:[14]

- Similar fingerprints should have similar hash values,
- Different fingerprints should not have similar hashes,
- Rotation and translation of the original template should not have a big impact on hash values,
- Partial fingerprints (with missing core and delta) should be matched if sufficient minutiae are present.

To compute a hash value and provide a data integrity, many algorithms are provided such as Message Digest 5 (MD5), Secure Hash Standards (SHA-1, SHA-256, SHA-384, and SHA-512), Message Authentication Codes (MACs), etc.

2.4 Related works

With the growth interesting of biometric authentication methods over traditional authentication methods, various biometric-based techniques are proposed by several researchers for provide a reliable user authentication. For instance, the techniques presented in [14, 15, 16, 17, 18, 19, 20, 21]. Other researches gone to make integration of biometric with data hiding methods (steganography and watermarking) to add additional level of security, for instance, the proposed algorithms in [22, 23, 24, 25, 26, 8, 27, 28, 29, 30]

3. THE PPROPOSED SCHEME

The proposed scheme is focused on providing a reliable authentication system by made a combination of biometrics features, hash function and steganography technique. The proposed scheme depends on comparing the entered user hashed fingerprint against the stored one in the system database. It works in two phases: enrollment and authentication.

- **Enrollment phase:**

Is the process of registered all the system users. The information of the system users was gathered by capture the biometrics features using a specific sensor, this information includes: user name, face image, and a hash value of the user fingerprint. This information are used to create a unique template for each user, these templates was stored in a system database.

The enrollment phase consisting of the following steps for each individual user to create a user template (Figure 5).

1- Acquire user face image ($cover_{face}$) from a sensor.
2- Acquire user fingerprint Fp from a fingerprint reader.
3- Extract fingerprint features Fp' using the minutiae point extraction methods. These minutiae points are used for determining the uniqueness of a Fingerprint.
4- Generate the hash value h_{Fp} of the Fp' using a hash function *H*, such as MD5 algorithm, as eq. 1.
$$h_{Fp} = H(Fp') \quad (1)$$
5- Store the resulted h_{Fp} with the associated user name in a database system as a user template.

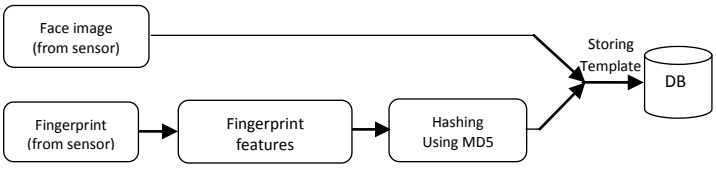

Fig -5: Enrollment phase

- **Verification phase:**

After the system user's templates are stored in the system database, he needs to undergo the verfication phase as shown in Figure 6.

In this phase, a comparison is made between the entered user's data and the template that is already stored in the system database from the first phase. The obtained result from the comparison process leads to the decision of verifying a person identity. This phase is done as the following steps:

1- The user is required to once again input his face image and fingerprint by a specific sensor for each one.
2- Repeat the steps 3 and 4 in the Enrollment phase.
3- Embeds h_{Fp} value in a $cover_{face}$ image using a steganographic technique, such as LSB method to produce a stego image ($stego_{face}$).

$$stego_{face} = cover_{face} + h_{Fp} \quad (2)$$

4- The system accepts the $stego_{face}$ image as the user identity, and then extract the hidden h_{Fp} value from it to compare it with the stored one for the same user in a system database. If matching is done, the user identity is authenticates and allow to login; otherwise, reject its identity.

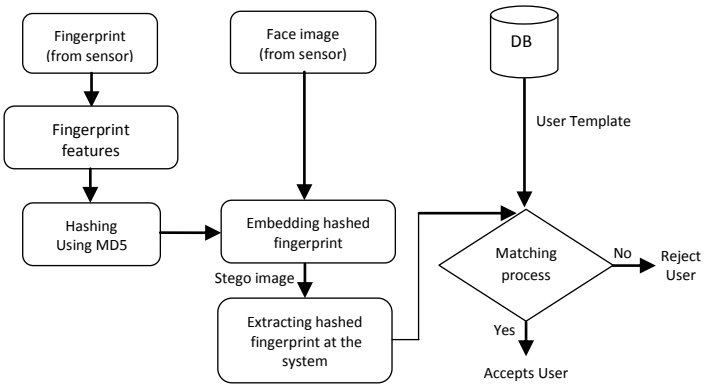

Fig -6: Authentication phase

4. SECURITY DISCUSSION

The proposed scheme provide number of security services such as:

- ***Authentication***: The proposed biometric authentication system serves to confirm the identity of a user; here we used a multimodal biometric (face and fingerprint) rather than using unimodal biometric, which provide more level of security. In general, goals of authentication include gaining of logical or physical access to an infrastructure (access control), or binding digital information to identities (information authentication). Access control mechanism encompasses many applications, from logical access to small personal electronic devices like memory storage devices secured by biometrics (e.g. Flash Memory drives protected by fingerprint verification), via user authentication for personal computers and computer networks to physical access control to buildings and areas. All of these access types can used the proposed system to provide a reliable user identification and authentication.
- ***Confidentiality***: Using steganography technique to hide the hash value of the user fingerprint provides more confidentiality of the proposed scheme, whereas, confidentiality is at the heart of what steganography does. The major role of the steganography to conceal the contents and existence of the secret data. For example, in case if any, unauthorized person try to fraud his identity to access to the system, he must replace the hidden authenticated user fingerprint hash value with his fingerprint hash value, and to get this data he must able to know where it are hidden in the stego image to can extract it.
- ***Integrity***: Because of the user fingerprint template is hashed, there is low risk of hacking or copying or fraud it. Protecting the integrity of the authenticated user fingerprint by using a hash function aims to ensure that once this data leaves the sender, no other unauthorized party can alter it, and any alteration in it will produce a different hashed fingerprint, this will cause to reject the user identity.
- ***Non-repudiation***: The user who verify his identity and allows to him to access to the system will not be able to deny any actions do by him later.

All of the these security services make the proposed scheme in this paper more appropriate and provide a high level of protection for user identification and authentication purposes.

5. CONCLUSIONS

Biometrics systems are gained more interesting over the traditional authentication systems, because it is available any time and the user not need to remember it, and moreover it is very hard to steal or fraud it

This paper suggest a reliable efficient multimodal biometric authentication system, using an integration between the user biometrics features, hash function and steganography technique. The proposed scheme is using face and fingerprint biometrics to achieve more reliable authentication. The biometrics face image and hashed fingerprint features of the users are collected and stored in the database system at the enrollment phase. Then, to authenticate any user, the system acquire the user face image and a fingerprint. The fingerprint features are extracted to use in computing a hash value using a hash function such as MD5 algorithm. The resulted hash value is embedding later in the user face image as a cover image using steganography technique like LSB, to produce the stego image which using to extract the hidden hashed user fingerprint features to compare it with the stored template. If the matching is done, the system authenticates the user identity, else the user identity is reject.

The proposed scheme provides number of security services such as authentication, confidentiality, integrity and non-repudiation. These security services make the proposed

scheme more secure against any attacks to fraud the user authentication.

REFERENCES

[1] S. Sadikan, A. Ramli, and M. Fudzee, "A survey paper on keystroke dynamics authentication for current applications", AIP Conference Proceedings, vol. 2173, 2019.

[2] S. Pin, Z. Ning, B. Andrew and C. Ke, "Recognizing your touch: towards strengthening mobile device authentication via touch dynamics integration", In Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia, pp. 108–116, 2015.

[3] R. Amin, T. Gaber, G. ElTaweel, and A. Hassanien, "Biometric and traditional mobile authentication techniques: overviews and open issues", Intelligent Systems Reference Library, vol. 70, pp. 249-264, 2014.

[4] G. Zheng, W. Yang, C. Valli, L. Qiao, R. Shankaran, M. Orgun, and S. Mukhopadhyay, "Finger-to-heart (f2h): authentication for wireless implantable medical devices", in IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 4, pp. 1546-1557, 2019.

[5] I. McAteer, A. Ibrahim, G. Zheng, W. Yang and C. Valli, "Integration of biometrics and steganography: a comprehensive review", Technologies, vol. 7, no. 2, 2019.

[6] K. Anil, R. Arun, and P. Salil, "An introduction to biometric recognition", Circuits and Systems for Video Technology, IEEE Transactions, vol. 14, no. 1, pp. 4–20, 2004.

[7] R. Arun, and J. Anil, "Biometric sensor interoperability: a case study in fingerprints", in: Biometric Authentication, Springer, pp. 134–145, 2004.

[8] A. Kapczyński, and A. Banasik, "Biometric logical access control enhanced by use of steganography over secured transmission channel", The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic, vol. 2, pp. 696-699, 2011.

[9] D. Peralta, M. Galar, I. Triguero, D. Paternain, S. García, E. Barrenechea, J. Benítez, H. Bustince, and F. Herrera, "A survey on fingerprint minutiae-based local matching for verification and identification: taxonomy and experimental evaluation", Information Sciences, vol. 315, pp. 67-87, 2015.

[10] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: a review", Symmetry, vol. 11, no. 2, 2019.

[11] W. Yang, S. Wang, G. Zheng, J. Chaudhry, and C. Valli, "ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures", The Journal of Supercomputing, vol. 74, pp. 4893–4909, 2018.

[12] Z. Akhtar and A. Rattani, "A face in any form: new challenges and opportunities for face recognition technology", Computer, vol. 50, no. 4, pp. 80–90, 2017.

[13] B. Schneier, "Applied cryptography: protocols, algorithms, and source code in C", Second Edition, Wiley Computer Publishing, John Wiley & Sons, Inc, 1996.

[14] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems", Pattern Recognition Letters, vol. 28, pp. 2427–2436, 2007.

[15] M. Khana, and J. Zhang, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", Neurocomputing, vol. 71, pp. 3026–3031, 2008.

[16] K. Barua, S. Bhattacharya, and K. Mali, "Fingerprint identification", Global Journal of Computer Science & Technology, vol. 11, no. 6, pp. 19-27, 2011.

[17] K. Habib, A. Torjusen, and W. Leister, "A novel authentication framework based on biometric and radio fingerprinting for the IoT in eHealth", In Proceedings of the 2014 International Conference on Smart Systems, Devices and Technologies (SMART), Paris, France, pp. 32–37, 2014.

[18] B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Towards secure cloud-centric internet of biometric things", In Proceedings of the 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), Niagara Falls, ON, Canada, pp. 81–83, 2015.

[19] P. Dhillon, and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services", Journal of Information Security and Applications, vol. 34, part 2, pp. 255–270, 2017.

[20] A. Pathan, K. Thakur, A. Chakraborty, and M. Kabir, "Fingerprint authentication security: an improved 2-step authentication method with flexibility", International Journal of Scientific and Engineering Research, vol. 10, no. 1, 2019

[21] P. Punithavathi, S. Geetha, M. Karuppiah, S. Islam, M. Hassan, and K. Choo, "A lightweight machine learning-based authentication framework for smart iot devices", Information Sciences, vol. 484, pp. 255-268, 2019.

[22] A. Jain, U. Uludag and R. Hsu, "Hiding a face in a fingerprint image", Proceedings International Conference on Pattern Recognition, vol. 16, no. 3, pp. 756-759, 2002.

[23] A. Jain, and U. Uludag,"Hiding biometric data", IEEE transaction on Pattern analysis and machine intelligence, vol. 25, no. 11, pp. 1494-1498, 2003.

[24] M. Vatsa, R. Singh, P. Mitra, and A. Noore, "Digital watermarking based secure multimodal biometric system", 2004 IEEE International Conference on Systems, Man and Cybernetics, vol. 3, pp. 2983-2987, 2004.

[25] H. Ihmaidi, A. Al-Jaber, and A. Hudaib, "Securing online shopping using biometric personal authentication and steganography", In Proceedings of the 2006 2nd International Conference on Information and Communication Technologies, Damascus, Syria, vol. 1, pp. 233–238, 2006.

[26] S. Katiyar, K. Meka, F. Barbhuiya, and S. Nandi, "Online voting system powered by biometric security using steganography", In Proceedings of the 2011 Second

International Conference on Emerging Applications of Information Technology (EAIT), Kolkata, India, pp. 288–291, 2011.

[27] H. Al-Assam, R. Rashid, and S. Jassim, "Combining steganography and biometric cryptosystems for secure mutual authentication and key exchange", The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), pp. 369-374, 2013.

[28] S. Kesharwani and N. Mehra, "Multimodal biometric image security using steganography and watermarking", International Journal for Scientific Research & Development, vol. 5, no. 10, pp. 835-840, 2017.

[29] M. Peethala, "Secure authentication system using biometric cryptosystem", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), vol. 13, no. 2, PP. 52-62, 2018.

[30] W. Yang , S. Wang, J. Hu, A. Ibrahim, G. Zheng, M. Macedo, M. Johnstone and C. Valli, "A cancelable iris- and steganography-based user authentication system for the internet of things", Sensors, vol. 19, no. 13, 2019.