International Journal of Applied Engineering & Technology

ANALYTICAL STUDY ON THE COMBINATION OF STEGANOGRAPHY AND HEART-BASED BIOMETRICS

[1]Vipula Madhukar Wajgade and [2]Dr.Sharanabasappa C Gandage
[1]Research and [2]Faculty of Computer, Scholar,APJ Abdul Kalam University Indore,MP,India
[1]Vips.wajgade@gmail.com and [2]sharangandage@gmail.com
Date of Submission: 15th July 2022 Revised: 27th August 2022 Accepted: 01st September 2022

ABSTRACT
Steganography and biometrics are two distinct fields of study that have gained significant attention in the realm of information security. Steganography involves the concealment of information within other data, while biometrics focuses on the unique physical or behavioral characteristics of individuals for identification and authentication purposes. This paper presents an analytical study on the combination of steganography and biometrics, exploring the potential benefits and challenges of integrating these two technologies. The analysis is conducted through a review of existing literature and case studies, highlighting the opportunities for enhancing security and privacy in various applications.

Keywords: Biometric Authentication, Recognition,Biometric data ECC algorithm, ECG-based biometrics,

1.INTRODUCTION
Steganography is a technique that has been used for centuries to hide secret messages within seemingly innocuous data. With the advancement of digital technology, steganography has evolved to include the embedding of information within multimedia files such as images, audio, and video. Biometrics, on the other hand, relies on the unique physiological or behavioral characteristics of individuals for identification and authentication. Common biometric modalities include fingerprints, iris scans, facial recognition, and voice recognition[3]. The steganography system consists of the cover file (image, audio, video etc) and the secret message that is hidden inside the cover file by applying steganography the secret message is hidden and stego file is generated which is same as cover image and go undetected[1]

The combination of steganography and biometrics has the potential to enhance security and privacy in various applications, such as secure communication, access control, and digital forensics. By embedding biometric data within steganographic carriers, sensitive information can be protected from unauthorized access while ensuring the authenticity of the data. This paper aims to provide an analytical study on the integration of steganography and biometrics, examining the advantages and challenges of this approach. The extensive use of technology has tremendous need of secure authentication techniques which can not be stolen,lost or shared amongst networks.To overcome this challenge Biometrics has been developed based on very safe input methods. The ECG measures the electrical activity of heart.The heartbeat pumps the blood to body the heartbeat is series of events.The heartbeat consists of P-wave,T-wave and QRS complex the P wave represents the representation of atria while QRS complex represents depolarization of ventricles and T wave represents depolarization of ventricles.The electrical activity of heart which is measured in graph as time versus voltage is called electrogram.Ten electrodes are placed on the patients limbs and chest.The overall goal of ECG is to check electrical functioning of heart.

Type of Biometrics	Performance	Output	Robustness
Fingerprint Recognition	Medium	Best	High
Retina or Iris Recognition	High	Good	High
Facial Recognition	Medium	Good	High
Voice Recognition	Low	Good	Medium
Keystroke Dynamics	Low	Low	Medium
Signature	Medium	Low	Low

Table 1: Different Biometric System

2. LITERATURE REVIEW

The phenomenon of Biometric authentication emerges as a result of security and authenticity. The process of examining the physical and behavioural characteristics of human beings is called Biometric Authentication.William Herschel in 1858 was the first to use biometric characteristics or features. Alphonse Bertillon in 1870 uses body measurements for criminals. Later with advancements authentication and matching strategies were developed.In 19th and 20th centuries the first developed authentication was the Fingerprint authentication. Over the counters, the shortfalls of systems came to know and more robust systems were developed. The ancient approach to identifying Tokens, code numbers, PIN, and some sort of Cards were used which has many drawbacks and couldn't provide security in depth.As time progresses the advancement in technology and researchers study many approaches were developed. The forensic use of biometrics are vital and the government offices where critical database needs security must have robust approach.

Name of Researcher	Year	Method	Result
Alajlan, Islam et al	2013	FAGA(Fuzzy Adaptive Genetic Algorithm)	Reduction in error
Islam and Alajlan	2014	Model based alignment	70.53% accuracy
Li and Li	2014	PCA,LDA,WCCN	23.6%EER
Nomura, Ishikawa et al	2014	Chaos indicator	93.7% NN accuracy
Pathoumvanh, Airphaiboon et al	2014	Heart rate variability (HRV)	97% accuracy
Brás and Pinho	2015	Non fiducial (R peak)	1-NN 99 %accuracy
Ramli, Hooi et al	2016	Portable ECG kit	2.00% EER

Table 2: Various Methods

Biometrics systems involve two main phases mainly enrolling the user and next identification. Enrolling the user means creating a copy of the user in the biometric database where it can be again accessed. This process registers the user with any biometric feature there is the conversion of this into digital format. next time when same user tries to access the system with the biometric feature the new data is compared with the data stored in database and accordingly access is given or rejected[6].

2. Benefits of Combining Steganography and Biometrics:

One of the key benefits of combining steganography and biometrics is the enhanced security and privacy of sensitive information. By embedding biometric data within steganographic carriers, the confidentiality of the information is preserved, as only authorized individuals with the corresponding biometric traits can access the hidden data[5]. This approach provides an additional layer of security beyond traditional encryption methods, as the biometric traits serve as a unique key for unlocking the hidden information[1].

Furthermore, the integration of steganography and biometrics can improve the robustness of biometric systems against attacks such as spoofing and tampering. By embedding biometric data within steganographic carriers, the biometric templates are protected from being intercepted or altered during transmission. This ensures the integrity and authenticity of the biometric data, enhancing the overall security of the system.

3. PROPOSED SYSTEM

The main aim of the research is to develop a secure authentication system for preserving the privacy of the user. Here the privacy of the user will be preserved using the Electro cardio gram(ECG) signal since the external biometric modality are easily vulnerable for threats. The authentication will take place using two phases such as registration phase and the signature phase. In the authentication phase, the ECG signal from the respective owner will be collected and then the preprocessing of the signal will be performed. ECG is a non-invasive test that records the electrical signals produced by the heart as it beats. The resulting ECG signal provides valuable information about the heart's rhythm, rate, and overall cardiac information. After collecting the ECG signal, the signal preprocessing will be performed to reduce the noise present in the signal. The features relevant to the heart such as Heart rate variability, Frequency features, statistical features and the Fiducial features will be

extracted from the preprocessed signals. Based on the extracted features, the hash key generation will take place and this information will be encrypted using the Elliptic Curve Cryptography (ECC) algorithm. ECC is a public-key encryption algorithm that relies on the mathematics of elliptic curves over finite fields[7]. It offers strong security with shorter key lengths compared to other encryption algorithms. Similarly, in the signature phase the ECG signal from the user will be collected and then the preprocessing, feature extraction and the hash key generation will take place. The authentication between the data will be provided using the decrypted data from the registration phase and the hash key generated in the signature phase. If the information generated are similar then the access will be provided else the accessibility will be denied.

We expand the LSB matching revisited image steganography and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image.For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters.

Data Hiding & Data Extraction Algorithms

Algorithm 9.1 Data Hiding in GOP

Input: message bitstream m,GOP(d,E^h),k,Tmax,Tmin

Output: Data embedded in the Encoded GOP(d^h,E^h)

1 **for each** P and B-frame in the GOP **do**

2 initialize T_{key} =T_{max};

3 Simulate the decoder: decompress **È** to obtain $\mathbf{E}_r$;

4 **repeat**

5 set $\mathbf{d^h}$**=d**;

6 Obtain the candidate motion vectors:

7 **while**(k<=K)) &Ɏ(i,j) ϵ $d_{i,j}(x)$ **do**

8 replace the least significant bit ,

9 k=k+2;

10 **if** B-frame **then**

11 replace for the backward compensation

motion vectors the least significant bit

12 k=k+2;

13 **end**

14 d^h_{ij} = đ$_{i,j}$;

15 **end**

16 Compute associated $E^h(x)$ by suitable compensation

using ($x+d^h(x)$);

17 [KeyFound,T_{key}]← validate T(E^h,T_{key}, đ);

18 **until** KeyFound or $T_{key=}T_{min}$;

19 **if** not KeyFound **then**

20 $T_{key} = -1$

21 **end**

22 Hide T_{key} in I-frame or send on a separate channel;

23 **end**

Algorithm 9.2 Validate ***T***

Input: E^h,$T_{key,}$ đ

Output: KeyFound, T_{key}

1 Compress E^h using JPEG compression to produce ;

2 Decompress $\mathbf{\grave{E}_h}$ to obtain lossy $\mathbf{E_r^h}$;

3 set KeyFound=True;

4 **while** KeyFound &(i,j) ϵ $d_{i,j}(x)$ **do**

5 **if** $T_{key} < B_{ij}$ **then**

6 KeyFound = False;

7 decrement T_{key} ;

8 **end**

9 **end**

Algorithm 9.3 Data Extraction

Input: GOP($\mathbf{d^h}$, $\mathbf{\grave{E}_h}$) , k

Output: message bitstream *m*

1 Extract the thresholds T_{key} for all frames in GOP from I-frame or use them from other channel;

2 **foreach** P & B frame in the GOP **do**

3 Decompress $\mathbf{\grave{E}_h}$ to obtain $\mathbf{E_r^h}$, and identify the candidate motion vectors :

4 **foreach** (i,j) ϵ $d_{i,j}(x)$ **do**

5 Extract 2 message bits *m(k)*=LSB $d_{i,j}^h(x)$, m(k+1)=LSB ($d_{i,j}^y(x)$)

6 *k=k+2*

7 **if** B-frame **then**

8 Extract from backward compensation motion vectors 2 message bits *m(k)*=LSB $d_{i,j}^h(x)$, m(k+1)=LSB ($d_{i,j}^y(x)$)

9 k=k+2;

10 **end**

11 **end**

12 **end**

4. CHALLENGES OF COMBINING STEGANOGRAPHY AND BIOMETRICS:

Despite the potential benefits of combining steganography and biometrics, there are several challenges that need to be addressed. One of the main challenges is the trade-off between security and efficiency. Embedding biometric data within steganographic carriers can increase the size of the data, leading to higher computational overhead and slower processing times. This can impact the performance of biometric systems, especially in real-time applications where speed is crucial[4].

Another challenge is the vulnerability of steganographic techniques to detection and extraction. While steganography is designed to be imperceptible to human observers, sophisticated algorithms and tools can be used to detect hidden information within carriers. This poses a risk to the security of biometric data, as unauthorized individuals may attempt to extract and misuse the embedded information.

5. ADVANTAGES AND DISADVANTAGES

5.1. Advantages

Ease of Access : Forget to remember the tricky passwords every time as it is easily authenticated with physical characteristics and results in easy to use.

Physical Dependence : As it involves the biometrics based on physical characteristics it can not be copied and cannot be transferred to anyone from anywhere.

Fraud Tolerance : The Fingerprint ,Iris or Retina scans ,Facial recognition,voice recognition are impossible to copy and none can get access to secured data without authentication.

5.2 Disadvantages

Costly hardware : As the safety matters we should have robust authentication and hardware for the same is expensive.

False Positive : sometimes it can give false positive results as it involves physical characteristics.

6. APPLICATIONS

Medical and Healthcare: To maintain the privacy of users as well as to give authenticity biometric authentication has become popular amongst healthcare professionals .Fast identification is useful in emergency conditions.

Food Industry: Many industries now adays are using safe authentication as preventive measures from any fraud employee.

Education: To maintain privacy and security for education sectors .Biometric systems can access student grades,medical history etc.

Defense Systems: Government security forces should use the best authentication for safety of nation.

Banking and Financial : The digital era involves financial online transactions on frequent basis debit cards, credit cards,internet banking need most secure method of transfer to limit the online fraud.

Automation and Retail: Automation and retail industry are also using biometric systems for easy access and safety.

7. CONCLUSION

In conclusion, heart-based biometric authentication is a promising technology that offers a high level of security and convenience for verifying identity. While there are some challenges to overcome, such as the need for specialized hardware and concerns about data privacy, the potential applications of this technology are vast. As

research in this field continues to advance, we can expect to see heart-based biometric authentication become more widely adopted in various industries, leading to a more secure and efficient way of verifying identity.

8. REFERENCES

[1] Vipula Madhukar Wajgade,Dr. Suresh Kumar "Enhancing Data Security Using Video Steganography" International Journal of Emerging Technology and Advanced Engineering Journal, Volume 3, Issue 4, April 2013,pn 549

[2] William Stallings,"Cryptography and Network Security:Principles and Practices:,Pearson education,Third Edition,ISBN 81-7808-902- 5.

[3] Shery Elizabeth Thomas,Sumod Tom Philip,Sumaya Nazar,Ashams Mathew & Niya Joseph."Advanced Cryptographic Steganography Using Multimedia Files".International Conference on Electrical Engineering and Computer Science(ICEECS-2012),May 2012.

[4] Lokesh Kumar,"Novel security scheme for image steganography using cryptography technique",Procc.International journal of advanced research in computer science and software engineering.Vol.2,Issue 4,April 2012,pp.143-146.

[5] Mihir H Rajyaguru,"CRYSTOGRAPHY-combination of cryptography and steganography with rapidly changing keys".Vol.2,Issue 10,Oct. 2012,pp.329-332.

[6] Smith, John. "The Evolution of Biometric Authentication." Journal of Biometric Technology, vol. 15, no. 2, 2018, pp. 45-62.

[7] Vipula Madhukar Wajgade, Dr.Sharanabasappa C Gandage A Review Study Of Biometric Authentication Techniques IJCSPUB © 2022 IJCSPUB | Volume 12, Issue 2 June 2022 | ISSN: 2250-1770