Securing Fingerprint Data using Huffman Coding Technique and Cuckoo Search based Steganography

Gnanaprakasam Thangavel, Santhosh J, Tigist Adam

Abstract*: Fingerprint plays an intelligent role in the authentication process. Even identical twins have same DNA but their fingerprints are unique. For authentication purpose, the financial sectors mostly decided fingerprint as their important authentication measure. Nowadays mobile phones also started to use fingerprint as one of the security tool rather than pattern or password. So securing the fingerprint in public environment takes lead role for the data owners. This research focused fingerprint security using Huffman coding technique and cuckoo search based Steganography. Huffman coding is used for lossless compression technique with respect to image data. Here fingerprint is available in the form of image data, so the loss of data could not be tolerated for authentication. Further, Cuckoo search is an optimization algorithm which is used to identify the best optimal solution from the group of results. Steganography is the best way of information hiding in internet. The key generated from the cuckoo search is embedding with the original fingerprint data. The best optimal security key is identified through cuckoo search. The key is shared with the user for the authentication process in the internet. This research implied the image compression technique, image encoding technique and finally verified the results with original fingerprint which proves no data loss and fingerprint data will be secure in the public environment.

***Index Terms*: Authentication, Cuckoo Search, Huffman Coding, Security, Steganography.**

I. INTRODUCTION

Steganography is the state of hiding the data into the image. Any form of digital media can hide into the image data. There are three kinds of Steganography methods available in the data security. Digital images, Audio and Video can be included in to the image data [1]. As audio, video, and other works become available in digital form, the ease with which perfect copies can be made, may lead to large-scale unauthorized copying which might undermine the music, film, book, and software publishing industries. In order to protect those publicly available data Steganography given support through watermarking. With the help of cryptography the public data will be secured [2]. Cover Object is the main tool of Steganography where the text data will be covered into the covered object. In this research, image Steganography takes higher place in order to provide maximum security. Digital images have finite set of picture elements called pels, pixels, or dots. There are various number of formats are available in images. Like JPG, GIF, BMP, TIF, PNG. Among the all BMP is suitable for the fingerprint operations. Although the fingerprint authentication technique is the dominant technology in the biometric sector, it may suffer attacks at different points during the authentication process [3]. Providing security is difficult in the internet. Cuckoo search helps to generate the secured key as the encryption parameter. CS mimics the obligate brood parasitic behavior of some cuckoo species in combination with the Lévy flight behavior of some birds and fruit flies [3]. From the above detailed discussion, It is better to take the Cuckoo Search for the optimized best key. Bit-map images are useful for the fingerprint image.

II. BACKGROUND STUDY

A. Research with Steganography

Security the data using Steganography will lead to the following issues, imperceptibility, payload and robustness [1]. The user's applications are deciding the technique which is suitable for the data security. Each issue is clearly discussed by Alla A Jabber in 2012. In the digital world, data security in the public environment is a tedious process. Steganography algorithms are classified by Cover Object, Domain, File Format discussed by Sumeet Kaur and Savina Bansal in 2014. Finally Steganography classified into, Image Steganography, Audio Steganography, Video Steganography, Text Steganography and Protocol Steganography [12].

In 2014, Shweta and Toppanavar [11] tried for online voting system using Steganography. Bio-metrics from the people are registered into the database. During voting, the duplicate person votes are identified easily. In this way they increased the security of the voting system using Steganography. In 2016, Chander Kant, Rajendar Nath [9] approached Steganography for Biometrics Security. Cryptography is not useful for image based security processing.

Revised Manuscript Received on June 14, 2019.

Gnanaprakasam Thangavel, Associate Professor, Department of Computer Science, Debre Berhan University, Ethiopia

J.Santhosh, Assistant Professor, Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,Avadi, Chennai, India.

Tigist Adam, Lecturer, Department of Information Technology, Debre Berhan University, Debre Berhan, Ethiopia

In their approach, secret key is added along with the image pixels. But high pixel (resolution) images are not efficiently utilized with their approach.

B. Research with Cuckoo Search

In 2009, Xin-She Yang and Suash Deb [8] formulated a new approach called cuckoo search (CS). CS used for solving optimization problems. CS is a nature inspired algorithm. The best result (key) or strongest (key) is the output of the algorithm. Cuckoos breeding behavior is the nature inspired. During validation, the computation always needs the best result with less execution time, in this aspect CS will produce the best optimal solution in the end.

In 2016, Mana Sopa and Niwat [4] developed an application for multiple choice constraints. The aim this research is regarding the hardware reliability and cost of the hardware. Identifying the reliability is tedious with the user's expectation and satisfaction. Towards cost, the people always expected high reliability for low cost. So the reliability and cost are directly proportional. Finally they decided CS has ability to produce the global optimal result in computation.

In 2017, Cai Zefan and Yang Xiadong [5] applied the Cuckoo search with the new diversity called Deep Search. Opposition based learning is difficult in deep search. Initially opposition based swarm used to identify the positions. But to find out the optimal best solution they used Cuckoo Search approach .

Mahbobe Bani and Mostafa Ghazizadeh [7] approached Cuckoo Search for Bayesian network structure learning in 2018. Bayesian network is a graphical model to represent the inference in unpredictable conditions. The structure of the network is a crucial one when network is named as Bayesian Network. In this approach, the acyclic graph is created like cuckoos, each graph has its own score called their fitness (strength), and final output will be the best optimal graph which is identified from Cuckoo Search Process.

C. Research with Huffman Coding Technique (HCT)

Huffman coding is developed by David A. Huffman in the year 1952. In computer science and information coding the role of Huffman code is very useful. Lossless data compression method is the best outcome from HCT. The output from the HCT can be viewed as variable length code.

HCT uses a specific method for choosing the representation for each symbol. Alphabets, Row and Column wise data are the input of HCT. Binary output is generated from the HCT output.

III. PROPOSED METHOD

The proposed method consists of data storage and data retrieval for authentication.

Fig. 2.1 shows the Data Storage of fingerprint image with security key generated from the Cuckoo Search. Fingerprint is available in the form of Bit-map image. Bit-map is converted into to pixel data with rows and columns. Cuckoo search generates the 64bit length key for the security purpose. Mixer is the process of encoding the Bit-map data and 64bit length key using Huffman Coding Technique. Quantization is the process of removing the errors during the encoding process. In the data storage part, the encoded image is stored into the public environment like cloud.

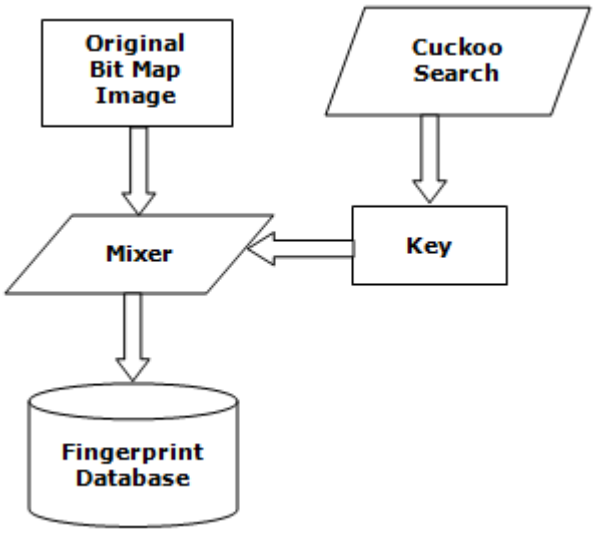

Figure 2.1 Data Storage

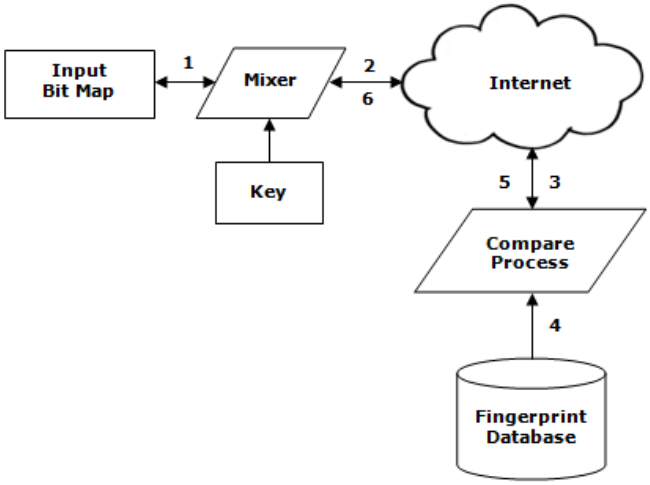

Figure 2.2 Data Retrieval for Authentication

The above Fig. 2.2 illustrates the Data Retrieval for Authentication process.

Authentication process follows the following Procedure 2.1. The result of the Authentication may be Success or Fail.

Procedure 2.1

Step1: Input from the User.
(Bit-Map Image is the input from User)
Step2: Mixes the Fingerprint with Key.
(Shared Key will be given as Input)
Step3: User's Current input
(Current input from the User for verification)
Step4: User's Old input
(Stored Data from the Fingerprint Database)
Step5: Comparison Result (True or False)
(Image

comparison)

Step6: Authentication Result (Success or Failure)

(If the wrong fingerprint or wrong key will lead authentication to be failed)

IV. IMPLEMENTATION

Securing fingerprint using cuckoo search based Steganography is implemented in Cuckoo Search process and Mixing process of Bit-Map image with Key. Finally the result will be stored into the Cloud Database.

A. Cuckoo Search

Cuckoo Search is an optimization algorithm. Also it is inspired from the nature. They are unique by obligate brood parasitism. The female cuckoo lays its egg in to the nest of other birds. The host bird never knows the brood parasitism of the cuckoo. This is nature's play. From this, the followings assumptions will come.

(i) The cuckoo lays only one egg (key) at a time into the random nest of host bird.

(ii) The best egg (strong key) from the quality nest will be forwarded to the next generation.

(iii) The host bird's nest is fixed, and the host bird can discover the cuckoo's egg with a probability.

The below output is generated in Windows 10 with JDK (Java Development Kit) 1.8 Version.

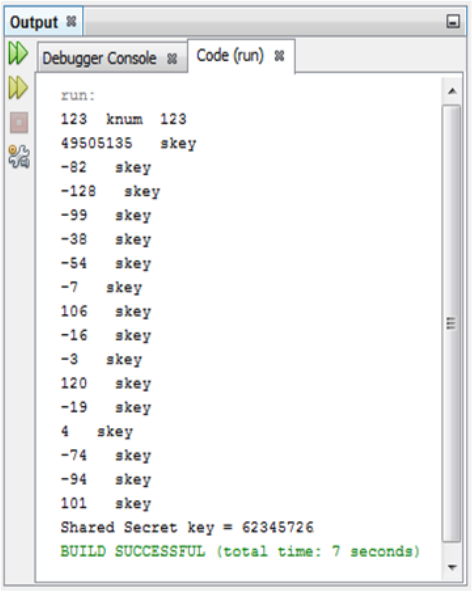

Figure 4.1 Cuckoo Search Key Generation

The above Fig.4.1 shows the screenshot, Cuckoo search generated security key to mix with the Bit-map fingerprint. The above code is executed with JDK1.8 (Java Development Kit) and Windows 10 operating system.

The final best key 62345726 will be given to the user, whenever the user tires for Authentication, user must give the secret key for mixing and produce the Authentication result. Authentication may failed because of the following reasons,

(i) If key may be forgot

(ii) If key may be lost

For the above cases, a new key will be generated from Cuckoo Search and given to the user. From the User end, User cannot update, edit or modify the key. The key should not be disclosed to any other third party. This is like ATM (Any time Money) PIN (Personal Identification Number). For one finger one key should be added, if some cases, Left and Right thumbs of same user can use the same key for storage.

B. Mixer

Digital devices gained the ability to display images in two types, Vectors and Bitmaps in Computer graphics. Bitmaps are composed by tiny rectangular cells called pixels. Each pixel is assigned a color, which is stored as a binary number.

Mixer carries the three major processes like DCT (Discrete Cosine Transform), Quantization, Huffman Encoding). In DCT the Bitmap images are converted to block form. Quantization is the processes of removing the unwanted data from the DCT output. DCT output may have the noise data, which will be removed through the quantization. Huffman encoding is used to strengthen the quantized data.

Fig. 4.2 illustrates the mixer processes, the digital signal conversion, error clearance, and security key mixing. The output image contains the fingerprint data with the cuckoo search generated security key. The output image is stored in the cloud for the future reference.

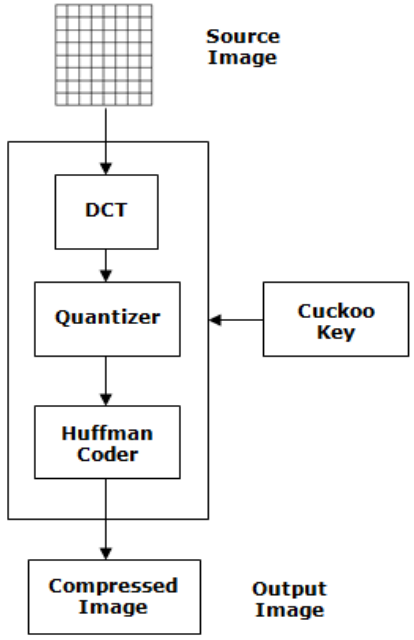

Figure 4.2 Block diagram of Mixer

The following procedure is used to convert the Bit-map image into blocks (8 x 8)

Procedure 4.1

for i=1,……M do

Choose one Cover-block b_i

$B_i = D\{b_i\}$

if $m_i = 0$ then

if $B_i (u_1, v_1) > Bi (u_2, v_2)$ then

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

swap B_i (u_1, v_1) and Bi (u_2, v_2)
end if
else
if B_i (u_1, v_1) < Bi (u_2, v_2) then
swap B_i (u_1, v_1) and Bi (u_2, v_2)
end if
end if
adjust both values so that | B_i (u_1, v_1) - Bi (u_2, v_2) | > x
$b'_i = D^{-1}\{ B_i \}$
end for

During the mixing process, fingerprint split into 8 X 8 pixel blocks; each block encodes exactly one message bit. The mixing process starts with selecting a pseudorandom block b_i which will be used to *i*th message bit.

Let $B_i = D\{ b_i \}$ be the DCT-Transformed image block.

Procedure 4.1 converts the Bit-map image into the pixel blocks. Followed by Quantization will process for remove the noise and Huffman coder will encode the key with the Bit-map pixel blocks. The final output from the Mixer is ready to store Bitmap image into the cloud database for the future reference of the user. It contains the encrypted image like security key and the original fingerprint image of the user.

V. RESULTS AND DISCUSSION

A. Fingerprint Data Compression

Usually image compression will lead a minimal loss of the original image, but using Huffman code there is no loss in the original image even after compression.

Table 5.1 Original vs. Compressed fingerprint data

Original Fingerprint Image in KB	Compressed Fingerprint Image in KB	De-Compressed Fingerprint Image in KB
86	80	87
110	101	109
135	128	134
156	150	154
210	202	211

The above Table 5.1 shows the compressed and decompressed fingerprint data. During Compression the amount of data will be reduced. The quantizer takes this work to remove the unwanted data in the input fingerprint data.

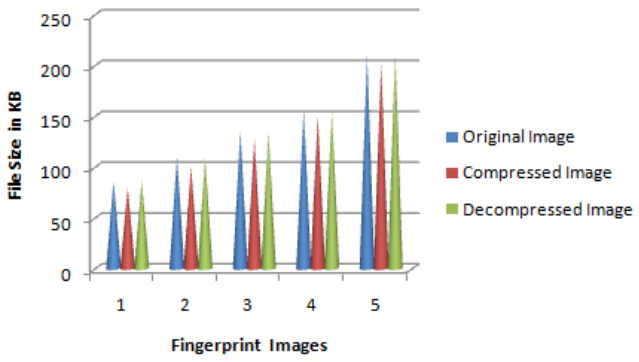

Figure 5.1 Original vs. Compressed fingerprint data

The above Fig.5.1 shows that there is No data loss during compression and decompression of the fingerprint data images. Quantization removes the unwanted data from the original data.

B. Encrypted Fingerprint Data

Mixer encodes the fingerprint data and secret key. During encryption there is some addition into the original fingerprint data. Secret key is 64bit length. There are different keys are generated by cuckoo search and added with different fingerprint images.

The following Table 5.2 shows the different fingerprint images embedded with different security keys. Fingerprint images are varies in size but the secret key lengths are same in size.

Table 5.2 Original vs. Encrypted fingerprint data

Original Fingerprint Image in KB	Encrypted Fingerprint Image in KB
86	96
110	121
135	142
156	163
210	221

The above Table 5.2 shows the security key added original fingerprint data. It occupies very less extra memory in the cloud.

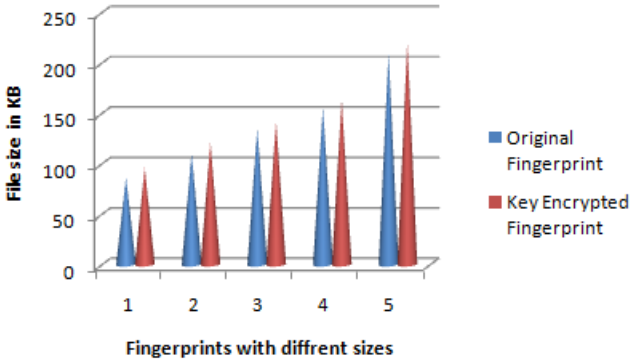

Figure 5.2 Original vs. Encrypted fingerprint data.

Fig. 5.2 depicts the memory usage of encrypted fingerprint data. The secret key generated by the cuckoo search having 64bit length which is encrypted with the original fingerprint data.

VI. CONCLUSION

In this paper, we have formulated a new approach in Steganography based fingerprint data security. The proposed method shows the effective storage of fingerprint data in public environment.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

During authentication process from third party, the user gives the secret key to validate the fingerprint data. Further, compression and decompression of fingerprint data with secret key makes no data loss is proved. For compression we used Huffman coding technique. As a result the security of fingerprint data is improved using this approach.

Huffman coding technique is used effectively in this research with black and white fingerprint image data. Future the user's photograph with color image may not be sufficient for Huffman Coding Technique. Cuckoo Search is generic and robust for many optimization problems. In this paper, the best optimal key is identified through cuckoo search. Future researchers can compare the efficiency with other optimization algorithms for their scope of the application.

REFERENCES

1. Alla A. Jabbar Altaay, Shahrin bin Sahib, Mazdak Zamani, An Introduction to Image Steganography Techniques, *IEEE International Conference on Advanced Computer Science Applications and Techniques*, Malaysia, 2013.
2. Rupali Jain, Jayshree Boaddh, *Advances* in Digital Image Steganography, *1st IEEE International Conference on Innovation and Challenges in Cyber Security*, India, 2016.
3. Narek Malkhasyan, Authentication based on Fingerprints with Steganographic data protection, *International Journal of Information Theories and Applications*, vol. 20, Number 3, 2013, pp. 289-294.
4. Mana Sopa, Niwat Angkawisittpan, An Application of Cuckoo Search Algorithm for Series System with Cost and Multiple choices constraints, *Proc. Science-Direct International Electrical Engineering Congress*, Thailand, 2016, pp. 453-456.
5. Cai Zefan, Yang Xiaodong, Cuckoo Search Algorithm with Deep Search, *IEEE International Conference on Computer and Communications*, China, 2017.
6. M. Mareli, B. Twala, An Adaptive Cuckoo Search Algorithm for Optimisation, *Journal of Applied Computing and Informatics*, vol.14, 2018, pp. 107-115.
7. Mahbobe Bani Asad Askari, Mostafa Ghazizadeh Ahsaee, Bayesian Network Structure Learning based on Cuckoo Search Algorithm, *Proc. IEEE 6th Iranian Joint Congress on Fuzzy and Intelligent Systems*, Iran, 2018, pp. 127-130.
8. Xin-She Yang, Suash Deb, Cuckoo Search via Levy Flights, *World Congress*, IEEE, 2009, pp. 210-214.
9. Chander Kant, Rajender Nath, Biometrics using Steganography, *International Journal of Security*, vol. 2, iss. 1, 2017, pp. 43-48.
10. Monica Adriana Dagadita, Data Hiding using Steganography, *IEEE 12th International Symposium on Parallel and Distributed Computing*, Romania, 2013, pp. 159-166.
11. Shweta A, Topannavar, Steganography based online voting system using bio-metric security, *International Journal of Advances in Science Engineering and Technology*, vol. 2, iss. 3, 2014, 59-62.
12. Sumeet Kaur, Savina Bansal, R.K.Bansal, Steganography and Classification of Image Steganography Techniques, *IEEE International Conference on Computing for Sustainable Global Development*, India, 2014, pp. 869-875.
13. Stefan Katzenbeisser, Fabien A.P. Petitcolas, *Information Hiding Techniques for Steganography, and Digital Watermarking*, Artech House, Boston-London, 2012.
14. Fu Gui-Xia, Gao Ming-Liang, An improved particle filter based on cuckoo search for visual tracking, *IEEE Chinese Control and Decision Conference*, China, 2018.

AUTHORS PROFILE

Dr. Gnanaprakasm Thangavel working as Associate Professor in Department of Computer Science, Debre Berhan University, Ethiopia. He has 9+ years experience in Teaching and Research. He has published papers in SCI (2), Scopus (2) and other refereed (5) journals. He presented more than nine papers in International and National Conferences including IEEE. He is the member of CSI and Life Member of ISTE. Network Security, Software Defined Networks and IoT are his research interests.

Dr. Santhosh Jayagopalan working as Assistant Professor in Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. He is having nine years of teaching and research experience. He completed his Ph.D in Network Security Specialization in Anna University. He has published and presented more than 10 research papers in reputed journals and conferences. His Research Interest include WSN, IoT, Network Security. Also he is the Life Member of ISTE.

Ms. Tigist Adam working as Lecturer in Department of Information Technology, Debre Berhan University, Ethiopia. Currently she is Dean of College of Computing, Debre Berhan University. Her research interest includes Network Security, IoT, Data Mining, and Robotics.