European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1245
http://eelet.org.uk

Secure financial transactions by using the picture-binding secret writing scheme

D. Saravanan
Faculty of Operations & IT, ICFAI Business School (IBS), Hyderabad,
The ICFAI Foundation for Higher Education (IFHE)
(Deemed to be university u/s 3 of the UGC Act 1956)
Hyderabad-India.

ABSTRACT-

Today, we are living in a technological world that streamlines our operations with a single click, making functions easier and more comfortable for users. One of the applications prevalent today is the hand phone, which offers enormous advantages and flexibility to users' lifestyles. It allows users to access information easily and conveniently, providing solutions to their needs. In addition to communication, hand phones serve various day-to-day functions such as browsing, financial transactions, health monitoring, and more, tailored to the user's preferences. These devices are capable of performing both character based and picture-based operations. In financial transactions, one of the security applications is undersized text-based correspondence. Through this, users receive one-time authentication services to complete desired operations. This not only enables users to complete specific tasks but also ensures that only authenticated individuals can perform particular operations. However, text-based communication is susceptible to hacking. In the proposed model, instead of character based authentication, users will receive picture-based authentication, hidden within the general message. To perform these types of operations, the technique of establishing hidden communications, called secret writing, is proposed here. It will overcome current methods and mitigate many security threats effectively.

Key terms: Charter based authentication, picture authentication, hidden correspondence, secret writing, Authenticated user, Hand phone, Flexibility.

1. INTRODUCTION

Today, technology allows users to perform various functions from their location, eliminating the need to physically visit functional units. Such applications are particularly effective in financial transactions, where users can conduct operations from their own locations, saving time, standing in lines, transport expenses, and more [1]. This not only saves time and costs but also facilitates additional operations more efficiently. Users are no longer constrained by the operating hours of financial institutions and can perform transactions anytime, anywhere. Commercial applications, such as those utilizing smartphones, enable quick and secure transactions with various authentication methods, including character-based or picture-based authentication. Currently, character-based authentication poses security risks, as hackers can easily intercept and manipulate character information [2]. Therefore, many service providers have shifted to picture-based authentication, where users select specific authenticated pictures, either in whole or in part, improving security significantly. This approach not only enhances security but also simplifies transactions for users, who no longer need to remember character-based information, only selecting specific pictures during transactions. Furthermore, advancements in technology now bind pictures with normal images, ensuring that unauthorized users cannot discern authentication methods, further enhancing security. The advantages of picture-based authentication have led to a widespread adoption of this method in financial operations, with most transactions now conducted through smartphones from users' locations [3]. This not only saves time and costs for users but also enhances convenience for service providers. These operations rely heavily on two crucial functional units: smartphone service providers and financial service providers, whose interaction ensures the efficient execution of transactions [4] Proposed smartphone-based transactions closely resemble traditional financial operations and are segmented into the following stages:

1. **Warnings and alarms:** This process will help the user to says the particular operation is done or the operations is aborted.

2. **Facts**: Facts of source of Information about the particular operations or functions will communicated to the user on regular intervals

3. **Implementation:** The implementation updating is communicated to user from the facility supplier.

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1245
http://eelet.org.uk

4. **Relocation:** Relocation is the process communicated to the customer particular transaction is successfully relocated form the user account to designated account.

To implement this type of service, users need a particular type of hardware and software setup, especially uninterrupted network service, to execute operations effectively. This technology allows users to reduce both time and costs, although they will require certain supporting equipment to complete operations effectively [5]. The entire operation is conducted through short-character-based or picture-based authentication. In both cases, any financial transaction is completed only after user authentication, ensuring that users perform certain operations securely and gain confidence that operations are conducted safely. In most cases, these operations rely on character-based authentication, which is a traditional and convenient mechanism. However, this technique has many drawbacks and flaws [6] As an alternative, today's technique, called hidden correspondence, employs picture-based authentication, allowing both users and service providers to communicate transactions in a concealed manner. This ensures that neither regular individuals nor hackers know the operations being conducted or the type of transactions initiated among the parties. Only authenticated users can complete transactions using the proper mechanisms.

During the implementation of hardware and software resources to achieve this technology successfully, users need to have the proper configuration to fulfil the above applications. For this, many user-defined protocols for communication are required [7]. Many existing protocols are used for specific applications and operations. One of the existing procedures is public key decoding. Users need proper technology and supporting functions. In this type of system, it will take more time for authentication and processing, leading to extra time for correspondence from either the user side or the service provider's side. Additionally, this requires highly configured network access; otherwise, it leads to more extra time. To avoid this complexity, in general, a symmetric type of authentication is proposed in the proposed technique compared to the existing technique. It never requires extra time for verification and processing. These specific system requirements will improve the correspondence between the client and the service provider, making the applications more effective and improving the time response[8]

Any communication among financial operators is done through proper authentication procedures, which can be either character-based or picture-based. Users receive one-time authentication on their devices during processing. Users are then directed to enter the received information in the appropriate place to complete the transaction. Based on the security mechanism, transactions are authenticated, and users can complete operations effectively[9] In the traditional technique, users expect to receive a one-time authentication message during the transaction, usually done through character-based or numerical-based inputs. Generating such inputs on the sender side is easy, and communicating the information does not require any extra hardware or software. Today, these inputs are generated with the help of computers, providing users with numerous input options based on their transactions. However, this existing technique is susceptible to tracking and hackers gaining access to this information. To address this drawback, our proposed technique generates and transfers high-security inputs into hidden pictures.

Any hacker who intercepts these inputs may also see the picture, but they will not have a clue that the image itself contains the secret code for the particular transaction. In the second stage of authentication in our proposed technique, the hidden message picture is not communicated directly to the user. Instead, the user receives only the corresponding link or source where the specific input information is available. Upon receiving the link, the user downloads the hidden picture message and completes the transaction[10]. Both on the banker's side and the receiver's side, proper techniques for converting the secret information in the image and proper recovery techniques to retrieve the secret information are communicated well in advance. During this two-way authentication process, it is very difficult for hackers to obtain the information effectively.

2. STEGANOGRAPHY

This procedure is one of the most familiar techniques for information sharing and communication. It allows users to transfer secret or confidential information effectively without third parties or hackers knowing the information. This technique is entirely different from other secret techniques. In the existing method, corresponding information is converted into an unreadable form and communicated to the receiver. Any hacker or person who knows the conversion technique can easily obtain the original information. However, using this technique, information is converted into an unreadable format and communicated to the user within a hidden object or source. Any hacker who gains access to the

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1245
http://eelet.org.uk

source will be unable to discern the hidden secret within the particular picture or object. They will only perceive the object itself, while only the authenticated user and receiver can access the hidden information. By using proper techniques, the information can be reconstructed and used by the intended recipients. Compared to existing techniques, this method not only converts information but also hides it effectively, communicating it to the users securely. Secrete writing method is entirely differ from the cryptography technique here information are converted and stored in the picture or any form, only sender will know this information's other really do not know what type of communication takes place between the sender and receiver. Only the authorized person only knows this secrete communications, but in cryptography modified source is visible to both sender and receiver.

Secret writing: As an alternative, today's technique, called hidden correspondence, employs picture-based authentication, allowing both users and service providers to communicate transactions in a concealed manner. This ensures that neither regular individuals nor hackers know the operations being conducted or the type of transactions initiated among the parties. Only authenticated users can complete transactions using the proper mechanisms.

Cryptography: It is the traditional technique where information is constructed into an unreadable format; only proper authentication or proper techniques help us reconstruct the original text or information. In this method, both parties will come to know how the information is embedded in the given file. By using the special functions or methods, the information is read by the parties.

73 110 32 116 104 105 115 32 112 114 111 112 111 115 101 100 32 119 111 114 107 32 112 114 111 106 101 99 116 32 116 104 101 32 109 101 115 115 97 103 101 32 105 115 32 104 105 100 100 101 110 32 105 110 116 111 32 116 104 101 32 74 69 80 71 32 102 105 108 101 32 98 121 32 117 115 105 110 103 32 116 97 103 115 44 32 116 104 97 116 32 105 115 32 44 32 104 101 114 101 32 119 101 32 117 115 101 32 60 109 115 103 62 32 38 32 60 47 109 115 103 62 32 116 97 103 115 44 32 84 104 101 32 74 80 69 71 32 102 105 108 101 32 105 115 32 101 110 99 111 100 101 100 32 105 110 116 111 32 98 121 116 101 32 102 105 108 101 32 97 110 100 32 116 104 101 110 32 105 116 32 105 115 32 99 111 110 118 101 114 116 101 100 32 105 110 116 111 32 116 101 120 116 32 102 105 108 101 44 32 98 121 32 116 104 105 115 32 116 104 101 32 101 109 98 101 100 100 105 110 103 32 111 102 32 105 110 102 111 114 109 97 116 105 111 110 32 119 105 108 108 32 98 101 32 109 117 99 104 32 101 97 115 105 101 114 46 32 84 104 101 110 32 116 104 101 32 60 109 115 103 62 32 60 47 109 115 103 62 32 116 97 103 115 32 97 114 101 32 101 109 98 101 100 100 101 100 32 105 110 32 116 111 32 116 104 101 32 99 111 110 118 101 114 116 101 100 32 116 101 120 116 32 102 105 108 101 32 97 110 100 32 105 110 32 98 101 116 119 101 101 110 32 116 104 101 115 101 32 116 97 103 115 32 116 104 101 32 110 101 101 100 101 100 32 109 101 115 115 97 103 101 32 105 115 32 101 109 98 101 100 100 101 100 46 32 84 104 101 32 116 97 103 115 32 119 111 114 107 32 97 115 32 102 108 97 103 115 32 111 114 32 99 104 101 99 107 32 112 111 105 110 116 115 44 32 98 101 99 97 117 115 101 32 105 116 32 105 115 32 117 115 101 100 32 116 111 32 100 101 99 114 121 112 116 32 116 104 101 32 109 101 115 115 97 103 101 32 102 114 111 109 32 116 104 101 32 112 105 99 116 117 114 101 46 32 65 102 116 101 114 32 116 104 101 32 101 109 98 101 100 100 105 110 103 32 111 102 32 116 104 101 32 60 109 115 103 62 32 60 47 109 115 103 62 32 116 97 103 115 32 97 110 100 32 109 101 115 115 97 103 101 32 116 104 101 32 116 101 120 116 32 102 105 108 101 32 105 115 32 116 104 101 110 32 99 111 110 118 101 114 116 101 100 32 105 110 116 111 32 98 121 116 101 32 102 105 108 101 32 97 110 100 32 105 116 32 105 115 32 99 111 110 118 101 114 116 101 100 32 105 110 116 111 32 116 101 120 116 32 102 105 108 101 46 32 87 101 32 99 97 110 32 110 111 116 105 99 101 32 116 104 97 116 32 116 104 101 32 74 80 69 71 32 102 105 108 101 32 97 102 116 101 114 32 101 109 98 101 100 100 105 110 103 32 105 115 32 110 111 116 32 99 104 97 110 103 101 100 32 97 110 100 32 116 104 117 115 32 103 105 118 105 110 103 32 110 111 32 99 108 117 101 32 102 111 114 32 116 104 101 32 111 102 102 101 110 100 101 114 115 32 116 111 32 102 105 110 100 32 116 104 101 32 104 105 100 100 101 110 32 109 101 115 115 97 103 101 46 10 10

Figure 1. Text converted in secreted writing code format(ASCII)

3. JPEG

In this proposed work project the message is hidden into the JEPG file by using tags, that is , here we use <msg> & </msg> tags, The JPEG file is encoded into byte file and then it is converted into text file, by this the embedding of information will be much easier. Then the <msg> </msg> tags are embedded in to the converted text file and in between these tags the needed message is embedded. The tags work as flags or check points, because it is used to decrypt the message from the picture. After the embedding of the <msg> </msg> tags and message the text file is then converted into

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1245
http://eelet.org.uk

byte file and it is saved as JPEG file. We can notice that the JPEG file after embedding is not changed and thus giving no clue for the offenders to find the hidden message.

Figure 2. JPEG containing secret writing content

4. PROCESS

The process of the proposed work can be described with the following block diagram

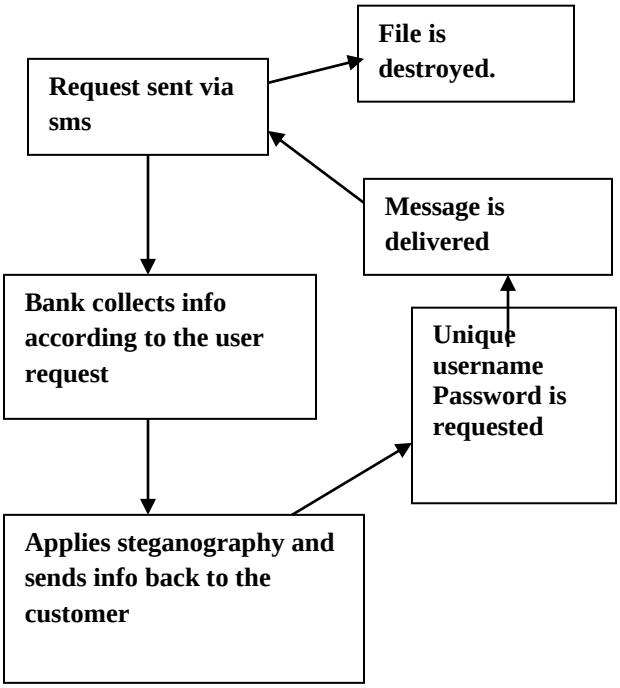

Figure 3. Proposed Architecture

In financial transactions, one of the security applications is undersized text-based correspondence. Through this, users receive one-time authentication services to complete desired operations. This not only enables users to complete specific tasks but also ensures that only authenticated individuals can perform particular operations. However, text-based communication is susceptible to hacking. In the proposed model, instead of character based authentication, users will receive picture-based authentication, hidden within the general message. This not only saves time and costs but also facilitates additional operations more efficiently. Users are no longer constrained by the operating hours of financial institutions and can perform transactions anytime, anywhere. Commercial applications, such as those utilizing smartphones, enable quick and secure transactions with various authentication methods, including character-based or picture-based authentication. Any hacker or person who knows the conversion technique can easily obtain the original information. However, using this technique, information is converted into an unreadable format and communicated to the

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1245
http://eelet.org.uk

user within a hidden object or source. Any hacker who gains access to the source will be unable to discern the hidden secret within the particular picture or object. They will only perceive the object itself, while only the authenticated user and receiver can access the hidden information

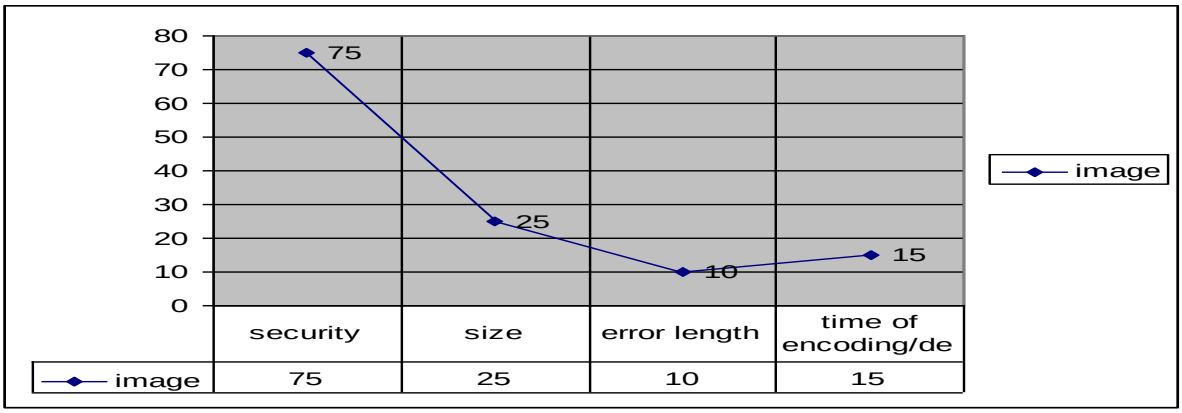

Figure 4 Graph image analysis

With the help of graph we analyze four major parts in the steganography they are Security of the message, Size of file, error made during steganography conversion and the time taken for steganography process. And we compare these features with different components which are used for steganography like Image, Video, Text, and Audio.

Figure 5 **Graph Video Analysis**

After the analysis we can see that the security of the video file is higher than the other three but the size is much bigger than other files so we can now ignore the video type. Next is the audio which has comparatively same security level but the size of audio is higher than other two and the error created during the process is much higher and so the audio is now ignored.

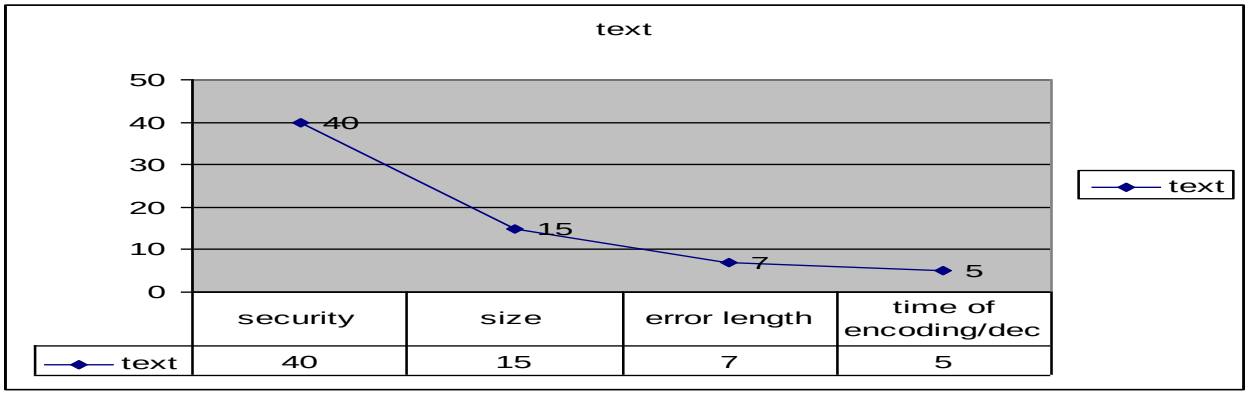

Figure 6. Graph Text Analysis

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1245
http://eelet.org.uk

Now we have the text file and the image file, in text file it is very easy to hide information and it is more easy to retrieve hidden information from text file than on an image, the time taken for the process of steganography is much smaller in text file than image file, but dude to the strength of security in text file it is ignored and hence we suggest that the image is probably the best way to hide information.

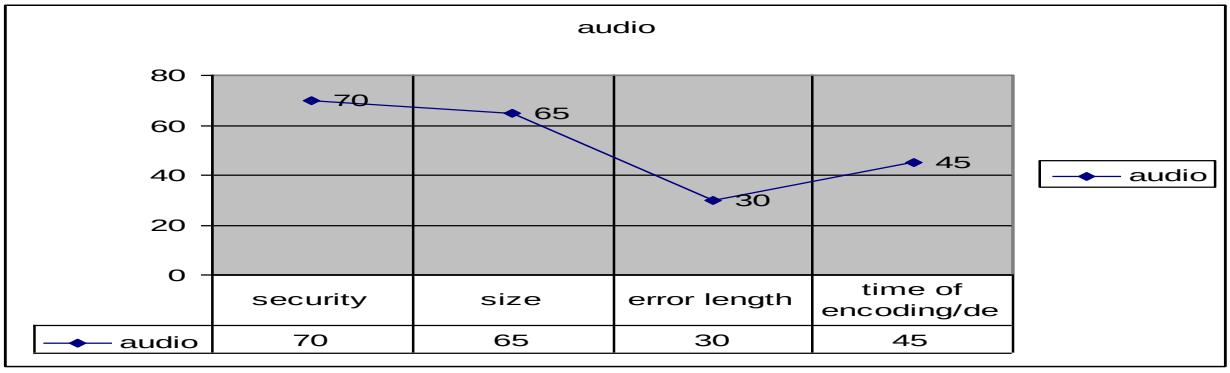

Figure 7. Graph Audio Analysis

5. WORKING PROCEDURE

The user is first registered to the bank's database, the user is asked to submit a picture of his choice in which his data will be transferred using the steganography method [5] shown in figure 8..After all the data are entered into the bank's database the bank will provide the customer with a unique mobile username and password, which is used for accessing the customers details in the mobile , shown in the figure 9.

Figure 8 User registration process

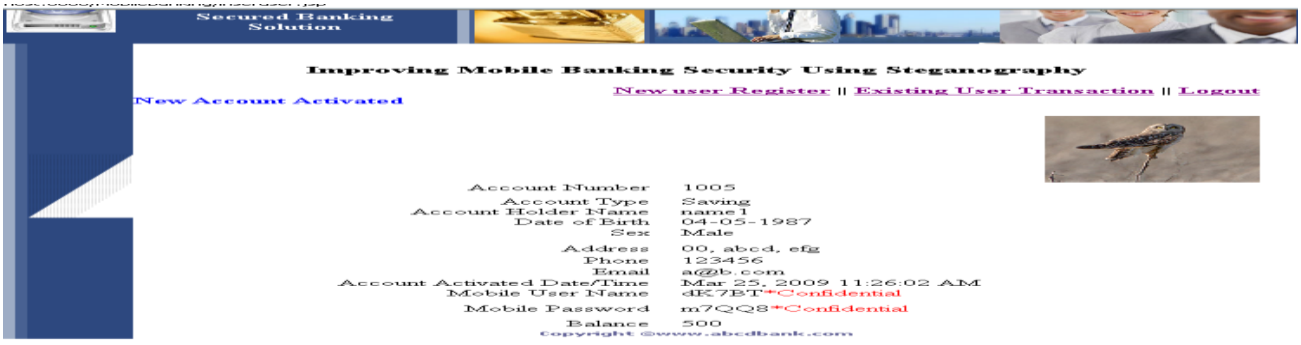

Figure 9. Getting the client information's.

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1245
http://eelet.org.uk

When ever the user wants to access his account to know about his balance after any transaction, they can use the unique password and username[6][7] and get the balance on their phone (figure 10, figure 11,and figure12)

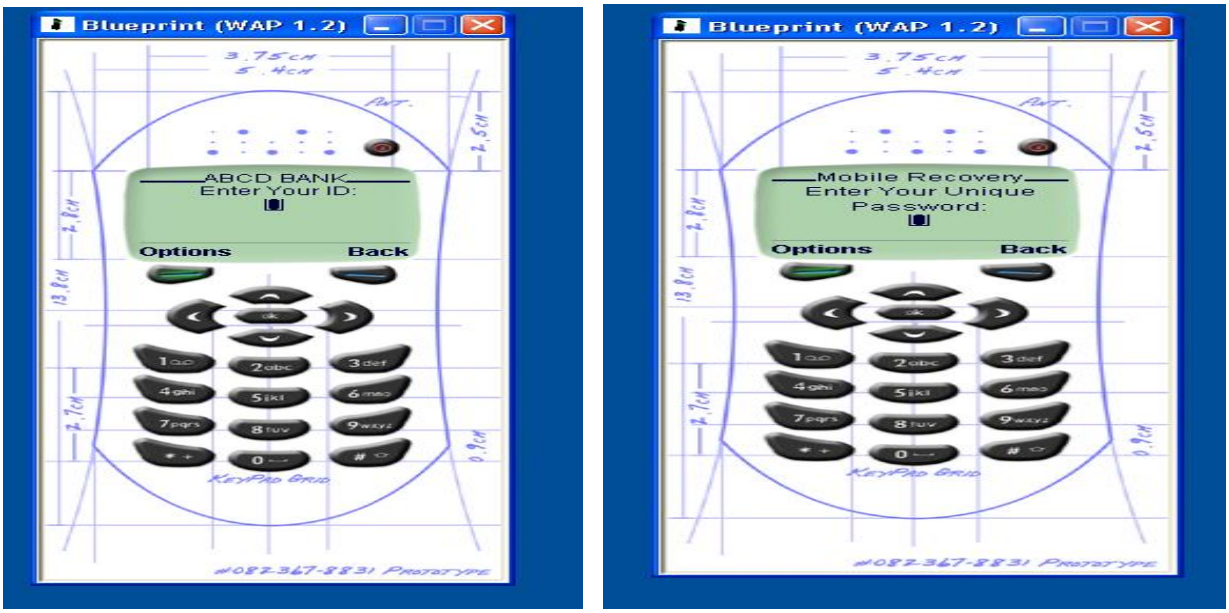

Figure 10,11 shown the character based alter information's

Figure 12 Contain character based secrete

The balance account is sent by using the steganography method by storing the data inside the image file given by the user.

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1245
http://eelet.org.uk

6. CONCLUSION

The advantages of picture-based authentication have led to a widespread adoption of this method in financial operations, with most transactions now conducted through smartphones from users' locations. This not only saves time and costs for users but also enhances convenience for service providers. The entire operation is conducted through short-character-based or picture-based authentication. In both cases, any financial transaction is completed only after user authentication, ensuring that users perform certain operations securely and gain confidence that operations are conducted safely. In most cases, these operations rely on character-based authentication, which is a traditional and convenient mechanism. the technique of establishing hidden communications, called secret writing, is proposed here. It will overcome current methods and mitigate many security threats effectively.

7. REFERENCES

[1] T. Laukkanen, "Comparing consumer value creation in Internet and mobile banking," International *Conference on Mobile Business (ICMB 2005)*, 11-13 July, 2005, pp. 655- 658.

[2] K. Pousttchi, and M. Schurig, "Assessment of today's mobile banking applications from the view of customer requirements," *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 5-8 January, 2004.

[3] D.Saravanan, Dr. Dennis Joseph, “Moving picture feature extraction using scheme pixel values methods”, Lecture notes on Data Engineering and Communications technologies, Volume 171, ISSN: 2397-4512, ISBN: 978-981-99-1766-2, Pages 739-748, doi.org/10.1007/978-981-99-1767-9_54, June 2023

[3] N. Kahzadi; E. Edalat.; and M. A. Dehgan-Dehnavi, "Commerce and M-Banking in World and Iran," *Proceedings of the Third National Conference on E-Commerce*, Tehran, Iran, 31 May-1 June, 2005, pp. 306-329 (In Persian).

[4] W. Itani, and A. I. Kayssi, "J2ME end-to-end security for Mcommerce," *2003 IEEE Wireless Communications and Networking*, vol.3, pp. 2015- 2020, 16-20 March, 2003.

[5] M. Shirali-Shahreza, "Stealth Steganography in SMS," *Proceedings of the Third IEEE and IFIP Int. Conf. on Wireless and Optical Communications Networks*, 11-13 April, 2006.

[6] M. Shirali Shahreza, "An Improved Method for Steganography on Mobile Phone", *WSEAS Transactions on Systems*, Issue 7, vol. 4, pp. 955-957, July, 2005.

[7] D.Saravanan, Dr. Vaithyasubramaniyan, Dr. Dennis joseph “Effective Utilization of image information using Data mining technique” , Intelligent systems reference library 172, Volume 172, Pages 207-215, ISBN 978-3-030-32643-2, Nov 2019.

[8] D. Saravanan, S. Vaithyasubramanian, “, Image encryption using matrix attribute values techniques”, Lecture notes in network and systems, 190, Pages 185-194, ISSN 2367-3370, ISBN 978-981-16-0881-0, July 2021.

[9] B. Dukic, and M. Katic, "m-order - payment model via SMS within the m-banking," *27th Int. Conference on Information Technology Interfaces*, 20-23 June, 2005, pp. 93-98.

[10] Saravanan, Shubhangi Urkude,”Confiscate Boisterous from color based images using Rule based technique”, Pages 503-514, Cognitive science and technology, ISSN:21953988, ISBN:978-981-19-2358-6, DOI: 10.1007/978-981-19-2358-6_47 , Jan 2023.