iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67986

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Enhancing Election Integrity: A Block-chain-Based E-Voting Solution

Dr. J. Senthil Murugan[1], Akshai Kumar T N[2], Danush S[3], Chandru K[4]

Abstract: ***To address the issues with the voting process, we suggest a novel and safe steganography based E2E (end-to-end) verifiable online voting system, despite the fact that there are already online voting systems available. By merging visual cryptography and image steganography, this study introduces a revolutionary method for online voting that improves system security without sacrificing system efficiency or usability. The voting mechanism will also have threshold decryption and password hashing. The program was created using web-based Java EE and integrates Glass fish as its application server and MySQL as its database server. Election officials and the election server are presumed to be reliable. Thirty representative participants completed a questionnaire survey to gather information about the software's user approval after it was built through usability and user acceptance testing.***

Keywords: visual cryptography, image stenographer, online voting system, usability testing

I. INTRODUCTION

A Brief Overview In elections, having a safe and effective voting process is one of the most crucial issues. Although an electronic voting system might be used to accomplish this, its speedier voting process than the paper ballot method by itself does not ensure its security. In order to gain the trust and confidence of users, electronic voting systems must be able to offer improved security measures without compromising usability, efficiency, or dependability. The user should have a certain amount of openness from the system without any privacy or trust violations. Electronic voting systems need to offer both universal and individual verify ability in order to meet this requirement. Individual verify ability refers to an electronic voting system's capacity to provide voters with vote verify ability through the use of vote receipts, while universal verify ability refers to the system's capacity to provide its users with election transparency.

These systems fall under the category of verifiable end-to-end (E2E) voting systems (Adida, 2008). End-to-end verifiability is a shift in electronic voting that enables voters to use the information supplied by the system instead of relying on the system to act appropriately, thereby testing the election's integrity (Ryan, Schneider & Teague, 2015). In this paper The eVote program is an enhanced E2E verifiable voting system that we propose in this work.This voting software may provide a voting system that is safe, dependable, practical, and effective. Our study goal is to use visual cryptography and image steganography in the system design to enhance the election process in an electronic voting system in terms of security and usability. Through user testing, we also hope to assess the established online system. The results of a test of an online voting system in the Canton of Zurich indicate that a more centralized infrastructure and more sophisticated technology are required (Beroggi, 2014). A homomorphic encryption-based electronic voting system is suggested in the paper (Azougaghe, Hedabou, & Belkasmi, 2015) to guarantee confidentiality and privacy. The use of steganography and encryption to safeguard data transfer during the election sets the eVote program apart from earlier online voting platforms. Data processing is when cryptography and steganography diverge from one another.

In terms of data processing, steganography and cryptography differ from one another.The ciphertext produced by cryptography and the stego-object produced by steganography are not visible to the human visual system (HVS). Because it provides a strong defense against threats, cryptography is a frequently employed approach in electronic voting. The authors present a novel method in this study that combines image steganography and visual cryptography to improve the security of the E2E Voting System.

Because image steganography can employ data sent over a network, it is chosen. According to Wang and Wang (2004), image steganography provides a solid answer for potential dangers and risks throughout the electoral voting process by protecting the message's existence as a secret. An enhanced and secure method is anticipated when these two strategies are combined (Morkel et al., 2005).

A mobile biometric-based design was presented by Petcu & Stoichescu (2015), utilizing methods including certificate keys, security tokens, and Secure Sockets Layer encryption. This is the format of this paper. In Section 2, the E2E verifiable voting system and associated works are discussed; in Section 3, the proposed eVoting system is discussed; in Section 4, the software testing and usability analysis are conducted; and in Section 5, the conclusion and limits are discussed.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

II. VERIFIABLE VOTING SYSTEM E2E

Nowadays, a variety of E2E systems have been put forth and are in widespread usage (Ryan et al., 2009; Chaum, 2004; Adida, 2008; Chaum et al., 2008; Hubbers, Jacobs, & Pieters, 2005). According to Burton, Culnane, and Schneider (2016), a verifiable voting system enables voters who are blind or live in remote areas to cast completely secret ballots in a verifiable manner. In theory, the E2E voting mechanism gives voters confidence in their vote.

For the purpose of verification, each voter receives a vote receipt for their encoded cast vote. Bulletin boards, a secure append-only broadcast medium, were used by E2E systems to facilitate this verification procedure. After voters finished the voting process, each encoded vote was placed on the bulletin board.

They must compare the values displayed on the bulletin board with the encoded value on their receipt in order to confirm the votes they cast. However, due to its encoding, the vote receipt cannot be used as evidence of vote purchasing or vote coercion. The E2E voting method would thereby safeguard voter privacy and promote incoercibility, maintaining the impartiality and integrity of the election outcome. Figure 1 shows this technique in action.

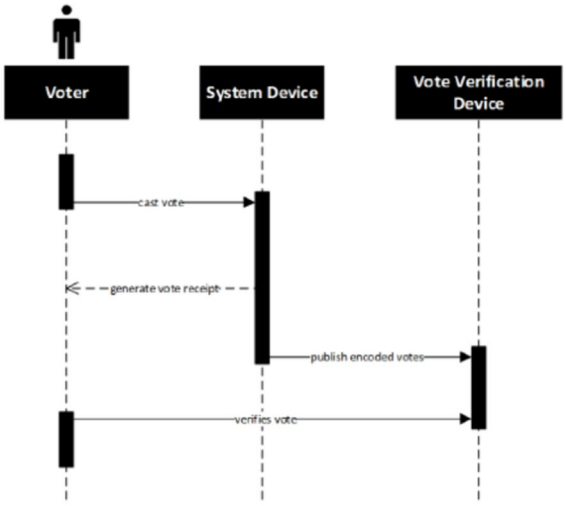


Figure 1: Mechanism of the basic E2E voting system

Prerequisites for Three E2E Voting Systems

For any electronic voting system to maintain its fundamental features—individual and universal verifiability—a number of requirements must be met. Most of these needs fall under the category of non-functional needs. For E2E verifiable voting systems in general, the following non-functional needs are listed (Fujioka et al., 1992; Benaloh, 2006; Gritzalis, 2002; Cetinkaya, 2008; Kofler et al., 2003; Aditya, 2005):

Completeness: All legitimate votes have been accurately counted.
Soundness: Voters cannot be swayed by dishonest voters.
Every vote must be kept confidential.
No voter may cast more than one ballot.
Voting is restricted to authorized voters only.
Fairness: The vote must not be impacted by anything. No one can reveal the total before the votes are counted, for example.
Verifiability: The voting outcome cannot be manipulated.
Robustness: Even if some voters or potentially some dishonest election officials falsify the results, the outcome accurately represents all submitted and properly formed ballots.
Even if voters are unreliable, they cannot obtain any knowledge about their secret ballots; this is known as incoercibility (the electoral process is assumed to be conducted by the voter in private).
Absence of receipts: No voter can create or get a receipt to demonstrate to another person the contents of their ballot.
Mobility: There are no limitations on the ballot-casting site.
Convenience: The system must, without sacrificing usability, enable voters to cast their ballots rapidly, in a single session, with little assistance or specialized knowledge.

A. *Related Articles on E2E Voting Mechanisms*

The security and adaptability of E2E voting systems differ. For a better understanding of E2E voting systems, this section will explore four distinct types of E2E voting systems that have been employed in medium- to large-scale real-world elections. These include the following: (1) the Helios voting system for the Université Catholique de Louvain Recteur election in Belgium; (2) the municipal election of Scantegrity II in Takoma Park; (3) the Princeton University Student Council election, which uses the Prêt à Voter system; and (4) the Rijnland Internet Election System (RIES) for the public election in the Netherlands (Carback et al., 2010). Verifiable online elections can be held using the open-source Helios Voting System (Adida, 2008). In contrast to a conventional election, when only election officials are permitted to observe during the election process, it was intended to guarantee a clean election environment through the open-audit election.

Its most recent version provides a more effective method of safeguarding the privacy of the system by designating a number of trustees, with the primary presumption that the trustees will be honest. Inspired by Benaloh's straightforward, verifiable voting algorithm, which used the Sako-Killian mix-net method and threshold decryption cryptosystem, this improvement was made. Every trustee must use cutting-edge cryptography methods to decipher the election's final total. Additionally, universal verifiability is guaranteed by an open-audit election. Through the employment of a ballot tracking center feature that allows users to confirm if their votes have been received and counted accurately, individual verifiability is achieved. The ciphertext format of this vote receipt is displayed to users.

By using a revolutionary method of printing confirmation codes on ballots in invisible inks, Scantegrity II improves election integrity in contrast to Helios (Chaum et al., 2008). It's a useful improvement on the original optical scan voting systems, Scantegrity and Punchscan. A voting portion plus a receipt portion make up the Scantegrity II physical ballot. Using a special pen that employs invisible ink, voters mark their preferred candidate on a typical paper ballot, just like in the traditional voting process. Thanks to this technology, voters can safely and discreetly save their receipts thanks to distinct confirmation numbers on each ballot that are impossible for hackers to compel. Only at the time of voting will voters be able to see the ballot's confirmation codes, which are kept confidential. There would be no way for anyone to obtain information about the confirmation codes prior to the voting. This feature allows Scantegrity II to gain the confidence and trust of the electorate, which leads to voter verification on an individual basis.

The method also guarantees that votes are neither removed or changed in order to rig the final tally of a given election and offers universal verifiability, allowing anybody to double-check the total's computation. By including invisible ink into its vote verification function, Scantegrity II could avoid some of the problems that Punchscan and Scantegrity brought up, such as randomization attacks and phantom votes. Additionally, Chaum released a paper on Secret-Ballot Receipt Election in 2004, which influenced Peter Ryan and his colleagues to create Prêt a Voter System (2009). Chaum also introduced Scantegrity II and its predecessors. It simplified the idea of Chaum's secret-ballot receipt system using the visual cryptography method suggested by Naor and Shamir (1994). To enhance voter turnout and reduce needless election expenses, the Prêt a Voter System was implemented to enable a quicker and more precise counting process.

Anyone using the system, including audit teams, can assess its integrity by examining various phases of voter verification, ballot preparation, and vote processing thanks to the election auditability feature. Verifiability is supported by this system on both a universal and individual level. As with previous E2E voting systems, Prêt à Voter guarantees that voters' ballots have not been tampered with. With each voter receiving a unique encrypted receipt, the votes were gathered and accurately counted in the tally. The only utility for this receipt is to verify the vote status against the read-only bulletin board; it won't leak out the ballot. Verifiability of the vote could be guaranteed with the help of certain security elements. Internal dangers can be foreseen and appropriately addressed with the help of these security techniques. Cryptographic techniques including threshold decryption cryptosystem, zero-knowledge proofs, homomorphic encryption, and others are included in the security components, along with encryption schemes like RSA, ElGamal, and Paillier. This would prevent the possibility of electoral fraud and keep the vote secret. Finally, we would want to talk about the Rijnland Internet Election System, or RIES. The RIES was created, like other E2E voting systems, to encourage more people to vote and reduce the needless expense of the traditional mail-in election (Hubbers, Jacobs & Pieters 2005). In order to finish his master's thesis, Herman Robers first created the system (Robers 1998). At the Delft University of Technology, it was subsequently put into effect during a local election. The Netherlands' Hoogheemraadschap van Rijnland, a local water management authority, soon followed suit. Eligible voters can use either of two methods to cast their ballots through RIES: electronically or by mail. local election in the Delft University of Technology. Soon after Hoogheemraadschap van Rijnland, a local water management authority in Netherlands continued its development. RIES allows eligible voters to cast their votes in two distinct techniques - either by mail or electronically.

This crucial component enables RIES users to independently confirm the election's outcome. In order to ensure that it offers internet voting in a clear, easy, and transparent manner without compromising the system's dependability, performance, and maintenance costs, the RIES voting system, which was used for the water boards election, differs from Robers' original one. They include the removal of the multifunction smartcard used for voter authentication, which was replaced by a digital secret key, and the installation of a feature that allows voters to vote by ordinary mail integration and more user types in the system. RIES is no longer used because of security issues discovered during deployment. The two primary goals of all E2E voting systems, as previously mentioned, were to provide universal verifiability and individual verifiability, commonly referred to as voter verifiability. Both features are present in all four of the voting systems under study. On the other hand, the authors are putting forth a brand-new E2E voting system that can meet all of the rules without sacrificing its usability, security, or integrity.

III. THE SUGGESTED SYSTEM

An enhanced form of the current end-to-end verifiable voting system is the eVote program. eVote is designed to support the voting process in small-to medium-sized elections, whereas the current E2E voting systems accommodate many election scales. In addition to providing a safe and dependable voting system, it also gives election administrators a platform that they may customize to suit their needs. Poll workers, voters, and system administrators are the three different categories (levels) of system users. Below is a description of its system and technological phases. Technology of Systems. The eVote voting system is designed to be accessed via a computer or tablet as a web application. The eVote's system architecture will use Java EE 6 because of its low platform reliance and other features including security, robustness, and scalability. An E2E Verifiable Voting System's development must prioritize security. The voting process in an online election depends on a number of cryptography-related information security building elements. The general defense of cryptography against electoral frauds such as ballot box manipulation and other attacks is the reason it is utilized. In addition, we present steganography as an adjunct to the cryptographic systems. Through the maintenance of confidential communication between two parties (client-side and server-side), steganography provides improved defense against threats and attacks akin to vote tampering. It serves to safeguard the information sent back and forth between the voter and the server, making sure that only the voters can access it. The system we propose uses image steganography. The following discusses the different technologies that have been utilized.

A. Hashed Password-based Scheme

When a person registers and authenticates, their password is secured using a hashed-based technique. According to Wagner and Goldberg (2000), it is cryptographically secure despite requiring little processing. The hashed value's ciphertext form cannot be reversed back to the original plaintext, thus hash-based methods are one-way operations. All that is needed for user authentication is for the server to check the hashed value that was computed from user input with the hashed value that was saved in the database. This protocol's techniques are complemented by salt value and key stretching to improve it and make it much harder to be penetrated by known attacks (such as dictionary and brute force attacks on stored pre-computed passwords). A trustworthy Pseudo-Random Number Generator (PRNG) is utilized to provide an entirely safe salt value. eVote was developed using the Java EE SecureRandom Class with a salt value of 24 bytes. However, by using dictionary or brute-force assaults on each hashed password, the hacker can still obtain the user's password even with the salt value increased. In order to strengthen the password, the PBKDF2 key stretching technique is implemented. This method is supported by the SecretKeyFactory Class in Java EE. This class uses the PBKDF2 function from RSA Laboratories' Public-Key Cryptography Standard (PKCS) #5 v2.0 to create secret keys. In Java documentation, this secret-key scheme is commonly referred to as PBKDF2WithHmacSHA1.

B. Seeing Cryptography

To avoid vote buying and selling and vote coercion, visual cryptography (Naor & Shamir, 1994) was used to give each voter a digital vote receipt that directly assured them. To create two shares of ciphertext, the plaintext—in this example, the ballot—will be encrypted. Pixel symbols are divided into two layers in the ciphertext. Java EE SecureRandom Class was used in the secret message distribution over the shares to offer an extra degree of protection to the ciphertext shares. Through the implementation of its Pseudo-Random Number Generator (PRNG) algorithm, SHA1PRNG, this class generates cryptographically robust random numbers. SHA-1 is the hash algorithm that serves as the PRNG's foundation. As a vote receipt, the voter will receive one share, while the other share will be kept in the database. These shares must be decrypted using a visual cryptography decryption technique. According to Chaum (2004), this system was taken from Chaum's secret-ballot receipt. The used mix-net approach employed by Chaum (2004) is modified simply because of its lengthy procedure.

C. Cryptosystem for Threshold Decryption

Threats and attacks cannot be prevented even with the use of cryptography-based security. In a remote electronic voting system, there are countless potential threats. As an extra degree of protection, the eVote program included a threshold decryption cryptosystem in addition to visual cryptography and a password hashed-based technique. The threshold decryption cryptosystem was created by Shamir in 1979. Key management for a cryptographic system is secure and dependable when a (k, n) threshold approach is used. It is possible to guarantee the security of a cryptographic system by having strong security and protection over the key management itself. Only authorized personnel would be able to access the vote tallying process thanks to the implementation of a threshold system in the ballot decryption step..

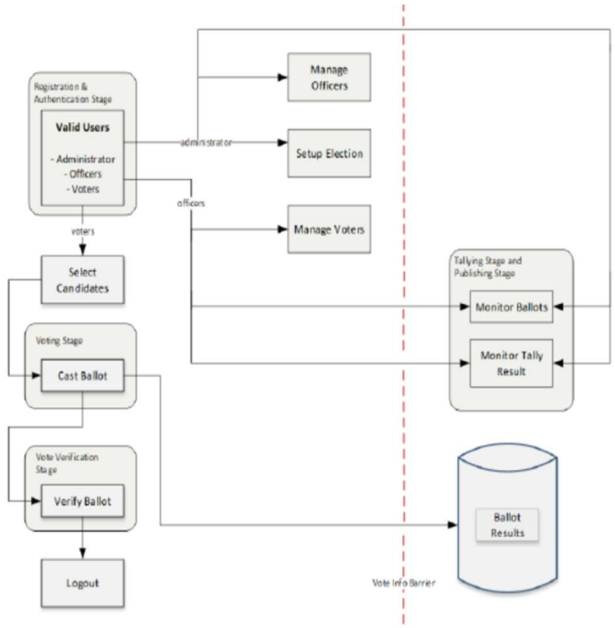
Before any election official or election administrator may access the summary ballot list, also referred to as the "ballot box," the private key, which has been split up and given to a select few appointed persons, must be combined in order to complete this decryption process.

D. Steganography using Images

Steganography is the study of concealing information during communication between two parties such that anyone in between would not be aware of it. Digital picture files are used as the cover file in image steganography, which offers an improved security method of data encoding. In comparison to other image steganography techniques, the F5 algorithm (Westfeld, 2001), as shown in figure 2, is thought to be more effective for secure data transmission, according to our earlier work (2011). F5 Steganography Algorithm message encoding procedure (Westfeld, 2001). In contrast to the other picture steganography algorithms—LSB, Palette-based, and Spread Spectrum—the F5 Steganography technique offers superior features. Comparing the initial and stego-image sizes for various image steganography algorithms was one of the evaluations carried out, and Figure 3 and F5 demonstrate that overall, the former looks superior.

Due to its modest size, the F5 stego-image can send the embedded stego-image to the election server more quickly (Rura, Isaac, & Haldar, 2011). The purpose of the other comparison is to assess how resilient each image steganography method is to statistical and visual attacks, specifically the Binary Similarity Measures (BSM) test and Regular Singular (RS) analysis, respectively. Initial and stego-picture sizes are compared across several image steganography technique implementations.It is evident from the data shown in Table I, which ranks the strength of each image steganography technique from low to high, that F5 is not particularly vulnerable to visual attack.

Additionally, F5 removes the potential for a Chi-square ($\chi 2$) assault (Bateman, 2008). The F5 picture steganography algorithm was selected for our system after taking into account Figure 3 and Table 1. In their publication, Fridrich, Goljan, and Hogea (2002) described how to break the F5 algorithm; however, Fard, Akbarzadeh-T, and Varasteh-A (2006) present a novel genetic algorithm (GA) method for secure steganography.



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

E. Stages of Voting

Vote verification in the eVote program, voting, tallying, authentication, and registration were the five steps of the electoral process. In Figure 4, the software's process flow diagram is shown. This is a more detailed explanation of every software step.

You are eligible to vote in this election. Please access the following page to register yourself and take note of the following details.

Election URL: https://localhost:8181/EVote
Election start date: 14/5/2013 8.30 AM
Election end date: 21/5/2013 5.30 PM

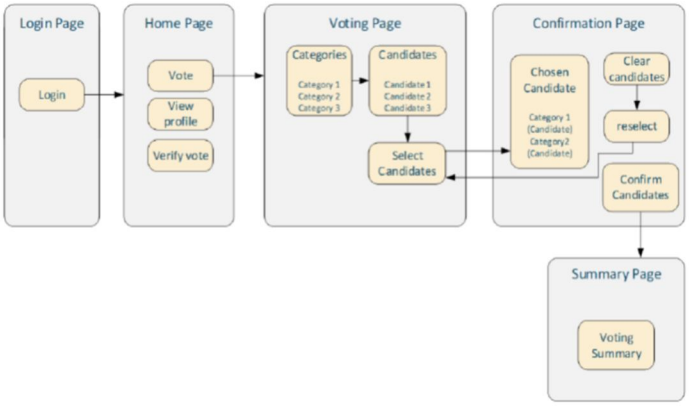
F. An image of the email that a qualified voter received

Input: message, shared secret,cover image
Output: stego-image
initialize PRNG with shared secret
permutate DCT coefficients with PRNG
determine k from image capacity
calculate code word length n<-2k-1
while data left to embed do
get next k-bit message block
repeat
G<-{n non-zero AC coefficients}
s<-k-bit hash f of LSB in G
s<-s+k-bit hash f of LSB in G
s<-s+k-bit message block
if s= 0 then
decrement absolute value of DCT coefficient Gs
inset Gs into stego image
end if
until s=0 or Gs=0
insert DCT coefficients from G into stego image
end while

You have successfully cast a vote in 'USA Presidential Election'

Attached is the your vote receipt, which can be used to verify your vote.

G. Mail confirmation of Vote Casting



H. Authentication Process

1) Stage of Authentication

In a distant electronic voting system, this step must be implemented. Ensuring voter identity is the aim of this step. By logging into the system, registered voters can verify their identity. To ensure their protection, they will be asked to enter their own login and password. The database only saves the hashed values of the user's passwords. For hash-based techniques, the hash values cannot be transformed back into plaintext because they are one-way functions. Comparing the hashed value generated from user input with the hashed value recorded in the database is necessary for the system to authenticate users. Following successful system login and identification as a registered voter, a user will be presented with a welcome screen.

2) Voting Phase

This step involves creating a secure electronic ballot and submitting it to the election server, which will gather and store all of the ballots. Following the completion of the two aforementioned steps, voters can access the voting page by logging in to the system. By choosing the candidates they like most for each category on that page, they can cast their vote. Every time the selected candidates are amended or evaluated, a new voter ballot is created. The voting screen is displayed in Figure 7, where voters can select one candidate.

3) Vote Confirmation

In a traditional paper-based voting system, authorized staff will declare the election's outcome after the tally procedure is complete. Voters will not be allowed to confirm their selections, though. Voters are therefore unable to be certain that their ballot will be counted as cast. The turnout in upcoming elections may be impacted by this.

4) Testing for Usability

Usability testing quantifies user concerns regarding the system. Nielsen (2012) states that usability is defined by five quality components: learnability, efficiency, memorability, mistakes, and satisfaction. The following nine out of ten usability heuristics principles for user interface design, which were created by Molich and Nielsen (1990), are used to analyze these five elements. System status visibility Consistency and standards Consistency between the system and the real world. Minimalist and aesthetically pleasing design; user autonomy and control; and assistance in identifying, diagnosing, and correcting mistakes Error prevention; recognition as opposed to memory; adaptability and effectiveness in usage.

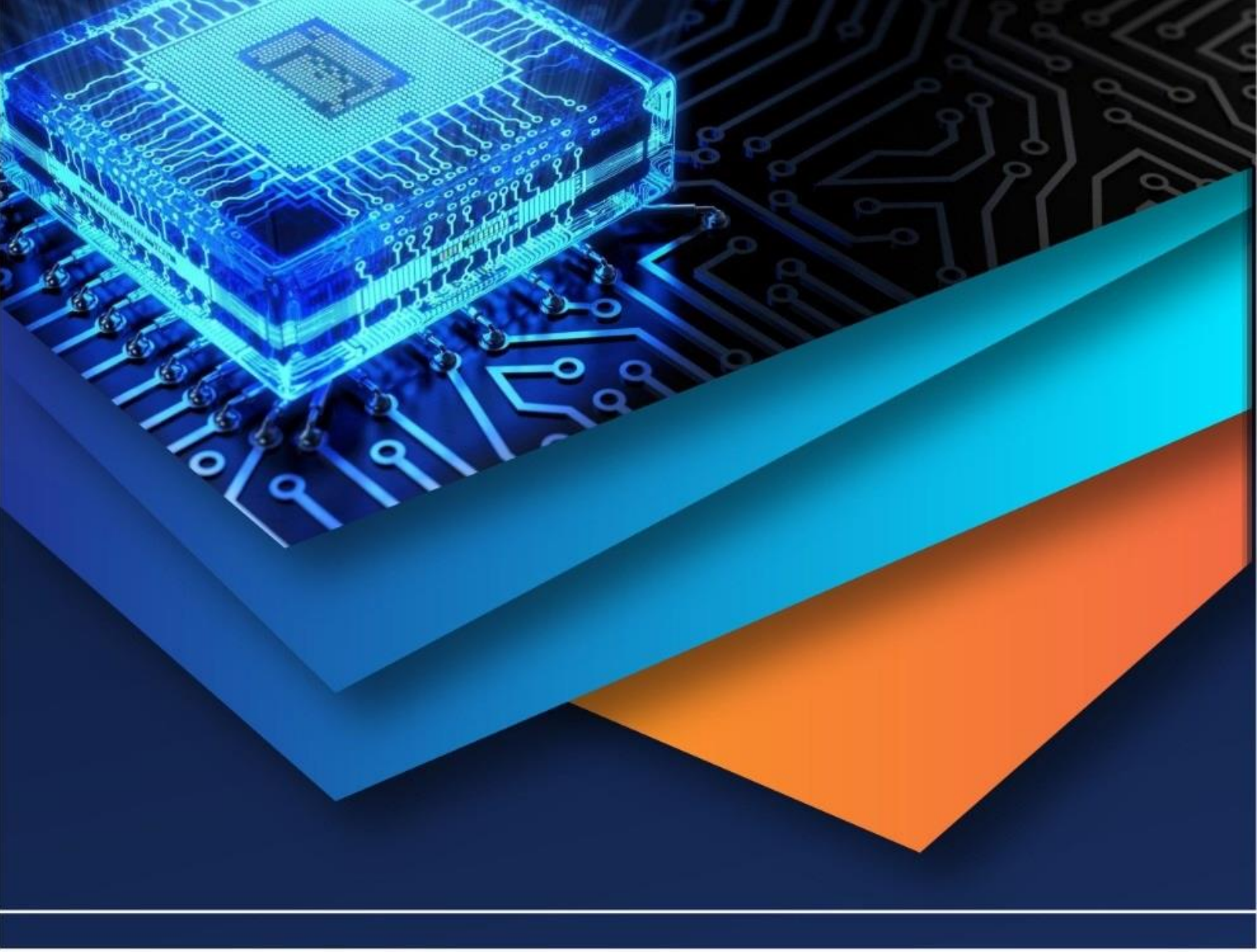
IV. CONCUSION

This work's primary contribution is the eVote software's ease of use and simplicity without sacrificing system performance, security, or efficiency. The voting system is powered by the following technology. During the registration and authentication stages, a password hashed-based system was used to protect user passwords. Visual cryptography was used to encode the ballot's plaintext into two ciphertext shares. The voter received one portion as their vote receipt, while the other portion was kept in the database. These shares were decrypted using a visual cryptography decryption technique. Additionally, it offers an enhanced system for receiving votes, and the vote verification function is the only way to accomplish this.

REFERENCES

[1] Apple Store Downloads 2016 | Statista—Statista.com. Accessed: Mar. 6, 2024. [Online]. Available: https://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/
[2] M. Pandey, R. Litoriya, and P. Pandey, ‘‘An ISM approach for modeling the issues and factors of mobile app development,’’ Int. J. Softw. Eng. Knowl. Eng., vol. 28, no. 7, pp. 937–953, Jul. 2018.
[3] P. Suresh and K. Gurumoorthy, ‘‘Mining of customer review feedback using sentiment analysis for smart phone product,’’ in Proc. Int. Conf. Comput., Commun., Electr. Biomed. Syst. Cham, Switzerland: Springer, 2022, pp. 247–259.
[4] A. Di Sorbo, G. Grano, C. Aaron Visaggio, and S. Panichella, ‘‘Investigating the criticality of user-reported issues through their relations with app rating,’’ J. Softw., Evol. Process, vol. 33, no. 3, p. e2316, Mar. 2021.
[5] Adida, B. (2008). Helios: Web-based Open-Audit Voting. In Proceedings of the 17th Conference on Security Symposium, USENIX Association, Berkeley, USA, pp. 335-348.
[6] Aditya, R (2005). Secure Electronic Voting with Flexible Ballot Structure. PhD Thesis, Faculty of Information Technology, Queensland University of Technology, Australia. Ambler, S.W. & Sadalage, P.J. (2006). Refactoring Databases: Evolutionary Database Design, Addison-Wesley Professional.
[7] Azougaghe, A., Hedabou, M. & Belkasmi, M. (2015). An electronic voting system based on homomorphic encryption and prime numbers. In Proceedings of the 11th International Conference on Information Assurance and Security (IAS), Marrakech, Morocco, pp. 140-145.
[8] Bateman, P. (2008). Image Steganography and Steganalysis, Master’s Thesis, Faculty of Engineering and Physical Sciences, University of Surrey, UK

[9] Benaloh, J. (2006). Simple Verifiable Elections. In Proceedings of the USENIX/Accurate Electronic voting Technology Workshop 2006 on Electronic Voting Technology Workshop, USENIX Association, Berkeley, USA, pp.5-5.
[10] Beroggi, G. E. G. (2014). Internet Voting: An Empirical Evaluation, Computer, 47(4), 44-50.
[11] Burton, C. Culnane, C. & Schneider, S. (2016). vVote: Verifiable Electronic Voting in Practice, IEEE Security & Privacy, 14 (4), 64-73.
[12] Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., Sherman, A.T. & Vora, P.L. (2010). Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy. In Proceedings of the 19th USENIX Conference on Security, USENIX Association, Berkeley, USA, pp. 19.
[13] Cetinkaya, O. (2008). Analysis of Security Requirements for Cryptographic Voting Protocols, In Proceedings of Third International Conference on Availability, Reliability and Security 2008, IEEE Educational Activities Department, Piscataway, USA, pp. 1451-1456
[14] Chaum, D. (2004). Secret-Ballot Receipts: True Voter-Verifiable Elections, IEEE Security and Privacy, 2(1), pp. 38-47. Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R.L., Ryan, P.Y.A., Shen, E. & Sherman, A.T. (2008). Scantegrity II: End-To-End Verifiability for Optical Scan Election Systems Using Invisible Ink Confirmation Codes. In Proceedings of the Conference on Electronic Voting Technology, USENIX Association, Berkeley, USA.
[15] Cronbach, L. J. (1951). Coefficient Alpha and the Internal Structure of Tests. Psychometrika, 16(3), pp. 297-334.
[16] Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), pp. 319-340.
[17] Fard, A. M., Akbarzadeh-T, M. R., & Varasteh-A. F. (2006). A New Genetic Algorithm Approach for Secure JPEG Steganography. In Proceedings of IEEE International Conference on Engineering of Intelligent Systems, Islamabad, pp. 1-6.
[18] Fridrich, J., Goljan, M. & Hogea, D. (2002). Steganalysis of JPEG Images: Breaking the F5 Algorithm. In Proceedings of the 5th International Workshop, IH 2002 Noordwijkerhout, The Netherlands, pp. 310-323. Fujioka, A., Okamoto, T. & Ohta, K. (1992). A Practical Secret Voting Scheme for Large Scale Elections. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, Springer-Verlag, London, UK, pp.244-251.
[19] Gritzalis, D. A. (2002). Principles and Requirements for a Secure E-Voting System. Computers & Security, 21(6), pp. 539-556.
[20] Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate analysis. Englewood: Prentice Hall International.
[21] Haynes, P. (2014). Online Voting: Rewards and Risks, Atlantic Council, Intel Security, Washington DC. Retrieved from http://www.mcafee.com/us/resources/reports/rp-online-voting-rewards-risks.pdf Hubbers, E., Jacobs, B. & Pieters, W. (2005). RIES — Internet Voting in Action. In Proceedings of the 29th Annual International Computer Software and Applications Conference, IEEE Computer Society, Washington DC., USA, pp. 417-424.
[22] Kofler, R., Krimmer, R. & Prosser, A. (2003). Electronic Voting: Algorithmic and Implementation Issues. In System Sciences Proceedings of the 36th Annual Hawaii International Conference, IEEE Computer Society, Washington DC., USA.
[23] Nielsen, J., & Molich, R. (1990). Heuristic evaluation of user interfaces. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1990, ACM, New York, USA, pp. 249-256.
[24] Morkel, T., Eloff, J. H., & Olivier, M. S. (2005). An overview of image steganography, In Proceedings of the Fifth Annual Information Security South Africa Conference in Sandton, South Africa, pp. 1-11.
[25] Ryan, P.Y.A., Bismark, D., Heater, J., Schneider, S. & Zhe Xia (2009). Prêt à Voter: a Voter-Verifiable Voting System. IEEE Transactions on Information Forensic and Security, 4(4), pp. 662-673.
[26] Ryan, P. Y. A., Schneider, S. & Teague, V. (2015). End-to-End Verifiability in Voting Systems, from Theory to Practice, IEEE Security & Privacy, 13 (3), 59-62.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY