ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =8.152, January-June 2025, Submitted in April 2025

A Study on Use of Cryptographic in Securing Online Voting System

Saurabh, Ph.D. Research Scholar, Department of Mathematics, Shri JJT University, Jhunjhunu, Rajasthan
Dr. Vineeta Basotia, Research Guide, Department of Mathematics, Shri JJT University, Jhunjhunu, Rajasthan

Abstract

Visual cryptography (VC) is a cryptographic approach that allows visual data, including text, images, videos, and more, to be prominently encrypted so that the decrypted data appears as a visual image. Electronic voting, often known as e-voting, is a voting method that is carried out online or using electronic means because it is simple to cast, count, and track votes in a way that is accurate, professional, and free from fraud. This paper compares and contrasts VC versus e-voting. Since I discovered some intriguing methods used, I will be creating a survey and review of all the current methods. We can also apply a new method to carry out the procedure. The most crucial methods that are combined for a significant search and survey are those like cryptography, steganography, and many more.

Key words: E-Voting, Security, Visual Cryptography, Techniques, Review

Introduction: -

Visual cryptography (VC) is a cryptographic approach that allows visual data, including text, images, videos, and more, to be prominently encrypted so that the decrypted data appears as a visual image. Visual secret keeping is a method that involves securely sharing the system. Instead of encrypting the data and storing it in a single location, it is being divided and then shared. As a result, there are multiple methods for protecting the data, such as dividing it into two or n shares and storing it in two different locations. As an illustration of all the papers I have seen, the majority of the writers permit two secret shares: one is stored in the voting system's database, and the other is maintained with the voter via email or while they are logged in to the system. This makes the system more transparent and makes it possible for it to function prominently. Since the shares function as them in this case, there is no ciphertext. Since little room is needed, VC is the expansion of the requirements that is carried out with the space. Due to the regulatory framework, it becomes completely secure and improves working efficiency. Patents from the 1960s provide some of the earliest examples of visual cryptography. Since VC functions as a greater development towards secure procedures to pay a larger impact of growth, it can be incorporated into a variety of systems.

Electronic voting, often known as e-voting, is a voting method that is carried out online or using electronic means because it is simple to cast, count, and track votes in a way that is accurate, professional, and free from fraud. This kind of voting uses a system that stores its data on a computer, which makes the counting process quick and error-free and also helps the system to continue. The procedure is referred to as online voting and better e-voting because fewer locations are sufficient, but the issue is that it can be abused and the system permits duplicate vote casting. Given that they incorporate the VC mechanism, the majority of current electronic voting systems are deserving of being operational. Steganography, encryption algorithms, VC, and decryption algorithms are a few more methods that are employed. In order to prevent natural forgery, a few more procedures and administrative involvement are incorporated in the system evaluation, which must be quite specific. Both lower and higher election forums can employ this kind of approach. Voters from outside the area can also cast ballots, which ensures that the correct candidate is chosen for the post. Voter and votee involvement should be provided in a way that is appropriate for legislation.

Online voting was used as an example of a survey that can support the system's future expansion. Votation.com, a private enterprise, was used by the Arizona Democratic Party to conduct their presidential primary online in March 2000. In this case, the system granted the user the ability to register for the poll, after which the user's credentials were sent to them via email or message for storage. As a security measure, the voter only needs to sit at home, vote using the correct information, and respond to a few questions. The user is directed to the voting platform to cast their ballot once their identity has been verified. However, in 2009, Estonia implemented a little more sophisticated feature that required only a few forms of identification and allowed anyone to enroll using them in order to prevent tampering. As a result, it was successful at the time. To prevent forgeries and multiple votes, all of these features were incorporated within the system.

A 2017 study found that it had no effect, according to the impact calculation. Two Swiss cantons took this action. According to the report, a study on "remote electronic voting and turnout in the Estonian 2007 parliamentary elections" focused on maximizing participation and digitizing the system to extend its storage capacity. With regard to the establishment of this system, the distinction between the upper and lower classes was eradicated. According to the report, this approach is totally unnecessary because those who were unavailable in 2007 are now fully available. However, because of the high turnout from those areas, the system was beneficial for individuals who lived in the wealthier areas during its implementation.

The researchers and those building the system should be careful to prioritize security as a result of the system's enumeration. The system's performance, cost-effectiveness, speed, and usability are all factors that should be considered when discussing user-friendly details.

Literature Survey:

Remote Voting System for Corporate Companies using Visual Cryptography:

This essay seeks to cast a vote while emphasizing the importance of protecting sensitive and important aspects of business choices. This specific approach is so adaptable that it permits voting from any distant location during times when important election participants are not accessible at work. Voting online, monitoring the system, setting appropriate security objectives, and maintaining transparency all contribute to the success of the task and produce accurate results. Twelve characters are randomly chosen from the available lowercase letters and digits, and they are encoded using a 64-bit key. The election server asks users to verify SSL certification by delivering them a valid Ki value. This type of protocol is adaptable and may be used to authenticate voters to election servers and the other way around. I've learned from this paper's outcome that voting systems need to be carefully considered, taking into account both security precautions and voting accuracy. The system should be verified to ensure that it offers the voter a dependable process with clear signals.

On the Development of Electronic Voting, A Survey:

A survey of electronic voting systems is included in this study, along with details on the system, benefits, and many other topics. It also includes a comparative analysis, highlights the most reliable current ones, and improvises the electronic voting method. As a result, there is greater interest in the security aspects of the selected system, which has a higher level of acceptance. Based on the system's previous security development, three weaknesses were identified. They are the social, sociotechnical, and technological divides. The goal and algorithm utilized in this specific paper are depicted in the graphic below.

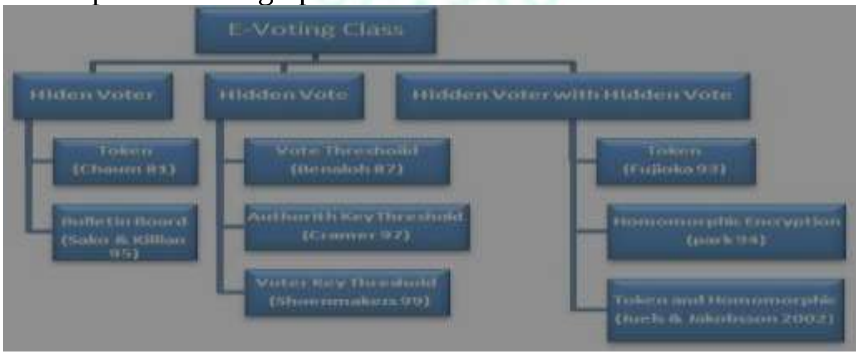
E-Voting Class
Hiden Voter
Hidden Vote
Hidden Voter with Hidden Vote
Token (Chaum 81)
Bulletin Board (Sako & Killian 95)
Vote Threshold (Benaloh 87)
Authorith Key Threshold (Cramer 97)
Voter Key Threshold (Shoenmakers 99)
Token (Fujioka 93)
Homomorphic Encryption (park 94)
Token and Homomorphic (Juels & Jakobsson 2002)

Fig 1: - Process of E-Voting in a survey written by the author Hutchison D.

Developing a Visual Cryptography Tool for Arabic Text:

This paper examines the Arabic language's exposure to the VC technique. The author claims that although Arabic has been the subject of numerous studies and research projects in VC, it has not received enough attention. Because Arabic is now widely used and holds great significance in many contexts, the author is focusing on applying VC techniques to it. In the Arabic context, the technology can also be used for digital signatures, online payment systems, watermarking, Captcha, electronic voting, anti-phishing, and biometric privacy. In contrast to English, which is written from left to right, Arabic is written from right to left. The Arabic letters appear intricate because they appear to be joined as they are being written or printed. Given the large number of Arabic-speaking internet users, the study found that recognizing and implementing the numerous developed techniques is valuable for maintaining the data's security and legibility. At the beginning, the canvas's image size is set as a function. The background color is set to white and the location is sketched. In order to embed and create the text in Arabic, it later invokes the make Text Image function. As the text is written, the image's placement is selected at random. The relatively modest number of participants was the limitation that was taken into consideration. This essay demonstrates how much the text's average time and efficacy have been acknowledged, along with its level of satisfaction. Additionally, the program is sophisticated and useful for real-world security tools like Arabic CAPTCHAs. In this sense, the study is also a better method of comprehending the language, which is becoming more and more popular due to its applicability.

A Novel Approach for Online Voting System using Visual Cryptography and Face Detection:

The benefits, drawbacks, and comparison of several electronic voting systems are covered in this study. It also suggests a method that gets over a problem where the VC can be added in addition to face detection since it can offer a better appropriate voting method that is more secure and user-friendly. People can vote from anywhere because they don't have to stand in lines, and they can avoid bringing their instincts if they can't vote because of work because it makes them feel drowsy. The system uses VC and face detection as algorithm techniques to obtain the most votes possible. A person can cast their ballot at home instead of traveling somewhere. Getting many, if not all, of the votes becomes simple. Therefore, the vote can be cast by whoever is most convenient. When safe algorithms are employed and voters are only permitted to cast one ballot, e-voting becomes secure. Security is provided, phishing attackers are avoided, and the number of fraudulent votes is reduced. The ease with which voters can cast their ballots online so pays dividends. Vote counting becomes incredibly simple. Voters are brought in through registration, which also gives identification for the process and enables voting to be done in a conspicuous manner. The administrator can only observe the results; their permissions are different from those of the user. Citizens cannot register for an electronic vote using false or inaccurate information.

Visual cryptography in internet voting for extended security:

The goal of this article is e-voting because it makes voting simple and automatic from any location inside the voting boundaries. Steganography and VC are employed to maintain confidentiality beforehand. Inside one image that is divided in two, a secret password is activated. The user can vote once they have correctly shared both images. Because it is secure and administrator permissions are distinct from user permissions, this system becomes easy to use. This makes it possible to cast a ballot without any issues from any location. Both large and small-scale elections are held because they aid in selecting the best candidate impartially. E-voting eliminates the inconvenience barrier because elections are limited to a certain location or area. This is being carried out with sufficient security and VC.

1. User registers.
2. Admin Checks and views with ID proof.

3. Valid is accepted otherwise rejected to vote.
4. User login with credentials, download security image.
5. User has to send it to email id and upload both the shares.
6. Admin checks again if it matches with the VC.
7. User votes, only once cannot vote again even if any mistake is done.
8. User logs out automatically and can view the result only once it is published.

As a result of this paper its design is being used in many large forums of voting. This particular system uses a two way client-server authentication process which provides more security. By this system people can cast vote from wherever they are. The VC technique used allows decryption visually as it becomes easier for the user. By this way it becomes more secure.

Online Polling System Using Extended Visual Cryptography:

This report presents advantages including cost efficiency and an increase in voter participation. It enables anyone to vote from any location while ensuring security. The VC methodology provides a more secure method for internet polling. The technology meticulously accounts for human characteristics. The voting procedure becomes more adaptable, allowing ballots to be cast from any remote location, even in the absence of the voter. This feature is offered by VC. It addresses human issues and security measures related to voting. It disseminates the confidential image during the registration process to establish security within the server. The VC approach is employed as a security mechanism. This technique permits the issuance of credentials to users, which the server accepts solely upon the entry of the proper ones for voting participation. This research reveals that the government allocates substantial funds for elections, although the percentage of voter turnout is rather low relative to the expenditure incurred. It presents an opportunity to mitigate fraud. The voting percentage can be elevated, and the expenditure can be diminished.

Online Voting System Using Visual Cryptography and Face Detection- A Survey:

This study analyzes the current e-voting systems, highlighting their disadvantages and advantages. It suggests a mechanism in which the VC is utilized in conjunction with face detection jointly. It also offers enhanced efficiency, suitable voting, and a user-friendly secure system. The current systems are plagued by issues such as privacy breaches, fraudulent votes, result manipulation, electoral disruptions, and ballot theft. Designed to be effective and efficient in enumerating the system as projected. The fingerprint voting system has evolved into an automated method of personal identification that facilitates verification and enhances security. Instead, facial identification utilizing VC is employed to facilitate and enable voting from any location. The secret sharing mechanism prevents any information from being disclosed. This paper discusses some notable technologies that can address voting processes. The effective mechanism of VC minimizes effort and enhances system fluidity. It additionally offers security and mutual authentication for the client and server concerned.

Anti-Phishing I-Voting System using Visual Cryptography:

This paper focuses on facilitating remote voting. A user may cast a vote via secure credentials. The password is generated with a VC approach. The election committee transmits two confidential keys: one for the individual and one for the system. Both a match and a vote can be cast. This pertains to the VC technique. It must be highly guarded and kept away from unauthorized individuals; otherwise, it will not be accepted. Phishing involves seeking personal information through various means. It primarily occurs via email or by spoofing by users whose information can be exploited on a fraudulent website. Network security has been expanding significantly. It is utilized for data access on a secure platform where administrative permissions are granted with appropriate credentials. Phishing is the illicit acquisition of private and sensitive information for nefarious purposes. Data obtained through phishing can be utilized in many forums in a fraudulent manner or discarded for the aim of a substantial monetary gain. A technique is suggested to avert and identify phishing. It is fundamentally predicated on anti-phishing. Image Captcha with the VC approach. Voting will be restricted to approved individuals to mitigate phishing risks. The server selects a text picture as the password for registration, which is subsequently utilized for login. The secret key must be disseminated. Therefore, utilizing the username and captcha can facilitate generation and mitigate phishing, contingent upon the authentication process conducted. The verification is complete and must be evident for the work to be classified as Anti-Phishing. The study employs the VC approach to mitigate phishing. Upon completion, it can be utilized in various large and small-scale settings. This enables secure voting to be implemented universally for casting ballots. The voter may cast their ballot only once and cannot redo it. The verification of its authenticity as opposed to it being a phishing attempt. The phishing website does not exhibit a picture if it is authentic. An intruder is prohibited from accessing the website, even with knowledge of the credentials.

Internet Voting System Utilizing Visual Cryptography: This research enhances security through the application of visual cryptography techniques alongside a secure password. The "ONLINE VOTING SYSTEM" is to be the most recent iteration. Voting is facilitated by the ability to cast ballots from any location. All data is securely saved on a well-maintained server. E-voting is simplified and engages a larger populace. It enhances user-friendliness and ensures reliability for voters. The VC technique is proposed. This system is offered for use in many locations, both low and high, due to its cost-effectiveness and excellent time management. It possesses a client-server architecture. The administrator and the user has distinct rights as necessary. Data is retained and deleted within the designated timeframe. This system can be utilized for corporate elections or governmental voting, facilitating ease of access for all citizens to participate in e-voting from any location, secured through the application of the VC approach.

Novel Authentication System Utilizing Visual Cryptography:

This work presents a comparative analysis of the visual cryptography approach against several parameters, including pixel expansion, number of shares, size, and quality of the reconstructed image. It enhances cost efficiency while maintaining a high level of security. Security is ensured, preventing any possibility of forgery. This method can also be applied in secure debit card systems. This technique aids in safeguarding against potential card fraud. This comprehensive strategy resembles the management by the CA and the bank. All authorizations are granted by the CA, and the bank accepts them; subsequently, each request from the bank is validated by the CA on behalf of the customer and processed for verification. This system incorporates the VC color approach, which was introduced to enhance security and mitigate counterfeit risks. This can be integrated into systems such as credit/debit cards and voting mechanisms.

Security of a Remote Voting System Utilizing Visual Cryptography and SHA:

The document presents a method enabling users to cast votes remotely. The implemented security measures are stringent. The encryption algorithm employed for the votes is AES, which is both secure and efficient. Time is conserved, and voting becomes more accessible with enhanced cost efficiency of the system. The Advanced Encryption Standard (AES) is employed for the encryption of votes. This technology expedites the vote storage procedure while also enhancing security. It offers a dual advantage in terms of performance and data retention. This technique enhances security while facilitating a substantial number of votes, albeit in a time-consuming manner. It undermines security robustness and is maintained in a secure manner. The system employs the VC technique and the AES algorithm to encrypt and robustly secure the data. The technique for remote voting is depicted in the graphic below.

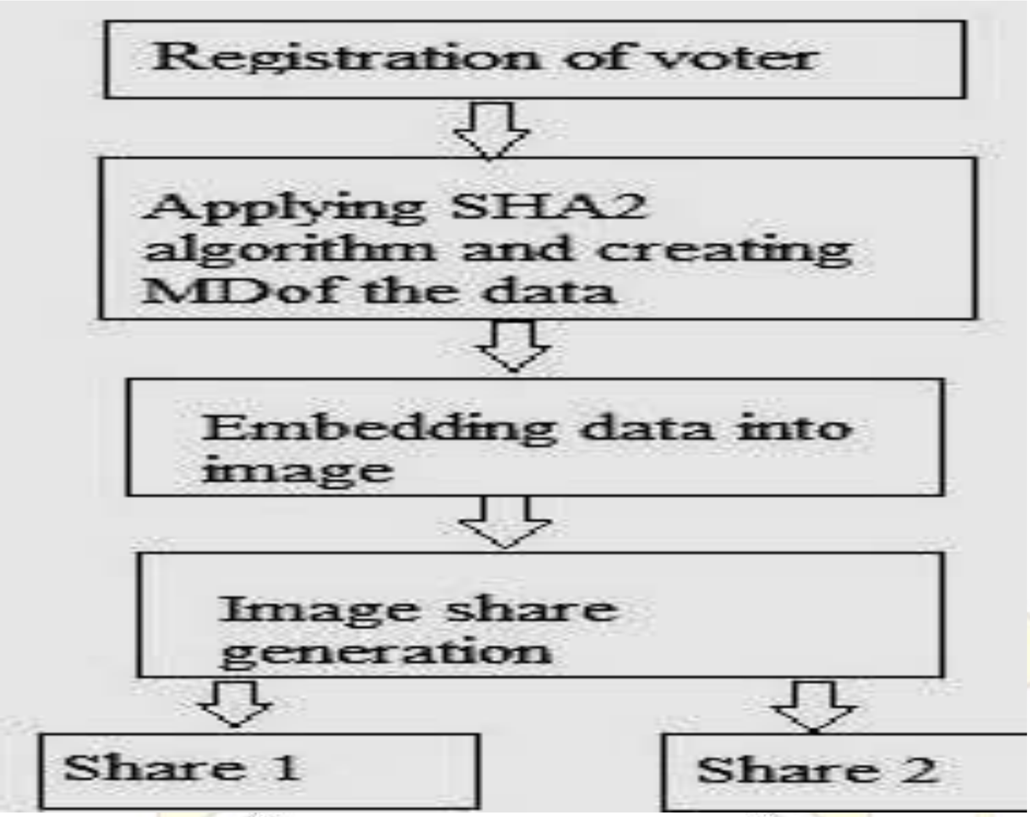
Registration of voter
Applying SHA2 algorithm and creating MDof the data
Embedding data into image
Image share generation
Share 1
Share 2

Fig 2: Process involved is security of remote voting system based on VC and SHA.

Electronic Voting System Utilizing Visual Cryptography Secure Multiparty Computation:

This study focuses on the identification evidence to be watched to detect and verify any forgeries, hence denying approval. A multi-party system is employed to provide security, reliability, and transparency inside the system. It also ensures that an individual is permitted to vote just once. The system comprises four phases: 1. voter enrollment, 2. voter authentication, 3. vote casting and recording, and 4. vote counting and election result dissemination. It establishes the framework for achieving optimal time complexity and seamless voting, facilitating participation from any location. Security is prioritized above all else. The system employs the VC approach and biometric methods to maintain authentication in a very relevant and structured manner. The process of constructing and reconstructing a biometric is unique to each individual, comprising two components. One is embedded on the voter's ID card, while the other is in the database; thus, both will be enabled only during a live process to prevent forgery. The employed algorithm does not permit reconstruction when only a single element is present. Security has a vital role here. The employed solution ensures that dual authentication methods safeguard both votes and voters from fabrication. It enhances the system by distributing data storage across several locations, hence facilitating traceability. Consequently, this technology is among the most modern and effective available.

This paper introduces a system that incorporates the method of Visual Cryptography with the Internet Voting System. It facilitates voting from any location and emphasizes the security protocols implemented to maintain system confidentiality. Access to the portal is permitted solely with the appropriate credentials. The password is formed by merging two shares (Black and White) using the VC approach. The system offers two shared secrets: one is assigned to the voter, while the other is stored in the launched database. Therefore, the voter must log in with the correct credentials to access the system and cast their vote. It is maintained securely to eradicate forgery and falsification within the system. The VC strategy employed to enhance system security is the 2 to 2 sharing mechanism, among several others. Even if one segment of the secret key is accessible, it does not facilitate the compromise of the system unless both segments are obtained. Therefore, this is one of the most secure methods for storing and retrieving votes from registered citizens. The employed VC approach is to verify the correct entity. The method and systems employed in this project enable individuals to vote from any location without disruption or inconvenience. The system is safeguarded and verifies identifying documents to prevent user falsification. Time complexity and cost efficiency have been regarded as factual considerations.

Verification of Online Voting Utilizing Cryptographic and Steganographic Methods:

This study introduces an e-voting system utilizing verification codes and steganography techniques. The user must enroll and will receive a comprehensive, step-by-step overview of the process; all information will be transparent and accurate. The technology ensures security while being cost-effective and time-efficient. This technique enables an individual to cast a vote from any permissible location. The system encompasses three primary processes that occur within it. The procedures include registration and identification, as well as the tallying and verification of votes. Eligibility is verified using the email address, and fabrication is prohibited. An end-to-end (E2E) voting system is developed utilizing the image steganography methodology based on DCT coefficients, which is superior to other available data hiding methods. This form of security is incredibly effective, leaving the forger bewildered in their search for the original data. Data is stored in numerous fragments and locations using VC, and is also maintained in an encrypted format. The proposed system has mitigated numerous vulnerabilities. It contributes to cost efficiency and enhances performance speed. Factors include trustworthiness, reduction in the utilization of additional hardware, specific device acquisition, installation, upgrades, and maintenance, all of which contribute to system security.

Execution and Assessment of a Steganography-Based Online Voting System:

This work, among the most recent and exemplary, incorporates many techniques, including end-to-end steganography and visual cryptography for enhanced security. The encryption employs a hash-based method, while the decryption utilizes a threshold-based approach. The performance and usability have been enhanced. Voters may cast their ballots from any location, as the restrictions will be implemented according to the officials. This is a client-server process in which a vote can be cast just once and exclusively by the registered user, as verification is required. Conversely, the server relies on the trustworthy environment to provide system accountability. The techniques of image steganography and visual cryptography are incorporated due to their enhanced security and the near impossibility of forgery. Three components of oversight are included: voter, polling officer, and system administrator. The security mechanism here differs from conventional cryptography, since it employs a stego-object instead of a cipher text, providing enhanced security. This system was initially subjected to a drill, followed by a survey, and subsequently implemented. Secondly, the system possesses two shared secrets, which are not stored in a single location; one is held by the user and the other by the server. Therefore, the system cannot be readily deceived. This renders the system user-friendly, secure, high-performing, cost-effective, time-efficient, and easily operable.

Graphs Depicted:

Two graphs are delineated below. The graphs pertain exclusively to papers 2, 5, 9, 13, and 15. This is due to the fact that these studies fall within the genre of comparative analysis and the evolution of the relative metrics employed in each graph. The voting system must implement these specific measures at an elevated level to facilitate comparison and application in real-time scenarios. Graph 1 illustrates the comparative metrics of the papers concerning performance, security, and usability. Conversely, Graph 2 illustrates the comparison of the standards of speed, cost, and visual cryptography associated with the specific articles. As they enter the category, they are compared and assigned a number ranging from 0, indicating the lowest, to 3.5, indicating the highest. Consequently, the graph is presented below:

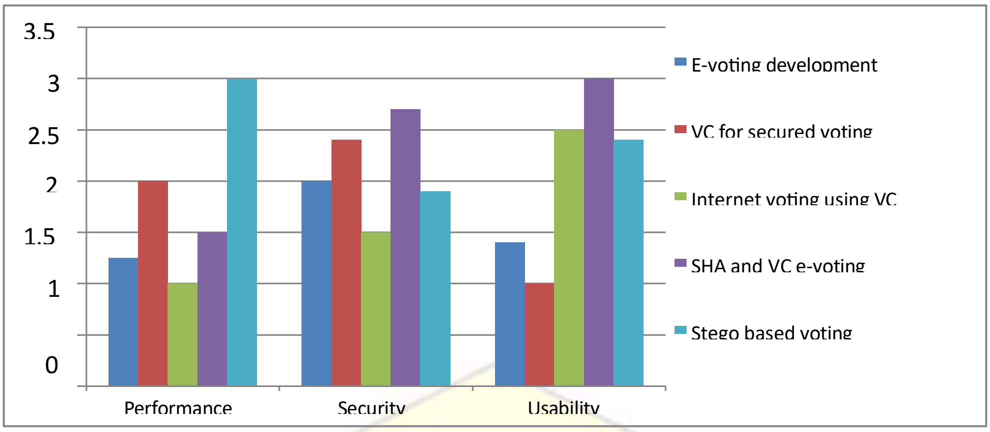

Fig 3: - Relative measures of the system.

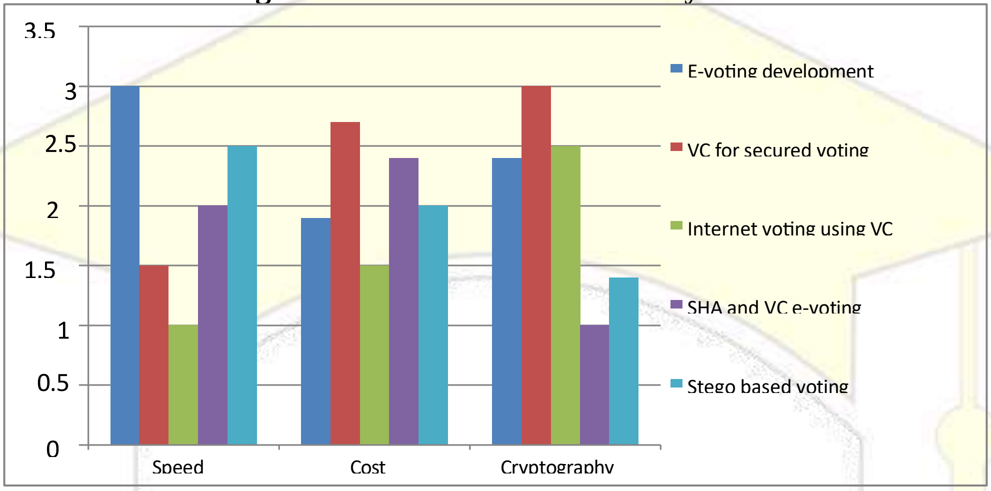

Fig 4: Comparison of the specific.

Factors Involved:

This particular table involves the factors that are involved in each paper and if the particular factor had been discussed in the paper it is checked to be yes, otherwise is checked to be no as it would not have been discussed. This gives a smaller comparative study of having the factors to be monitored in every paper that are discussed.

Title	Performance	Speed/ Time	Cost	Security	User Friendly	Usability	VC	Other
Remote Voting System for Corporate Companies using Visual Cryptography	No	No	No	Yes	Yes	No	Yes	Yes SSL
On the Development of Electronic Voting: A Survey	No	Yes	No	Yes	Yes	Yes	Yes	No
Developing a Visual Cryptography Tool for Arabic Text	No	No	No	Yes	No	No	Yes	No
A Novel Approach for Online Voting System using Visual Cryptography and Face Detection	Yes	No	No	Yes	Yes	No	Yes	Yes Phishing
Visual cryptography in internet voting for extended security	Yes	No	No	Yes	Yes	Yes	Yes	Yes Steganography

Online Polling System Using Extended Visual Cryptography	Yes	No	Yes	Yes	Yes	No	Yes	No
Online Voting System Using Visual Cryptography and Face Detection- A Survey	Yes	Yes	No	Yes	Yes	No	Yes	Yes Face Detection
Anti-Phishing I- Voting System using Visual Cryptography	No	No	Yes	Yes	Yes	No	Yes	Yes Phishing, Captcha, NS
Internet Voting System using Visual Cryptography	Yes	No	No	Yes	Yes	Yes	Yes	No
Novel Authentication System Using Visual Cryptography	No	No	No	Yes	Yes	No	Yes	No
Security of Remote Voting System based on Visual Cryptography and SHA	No	Yes	Yes	Yes	Yes	No	Yes	Yes AES
E-Voting System Using Visual Cryptography Secure Multi- party Computation	Yes	No	No	Yes	Yes	No	Yes	No
Visual Cryptography in Internet Voting System	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Online Voting Verification with Cryptography and Steganography Approaches	Yes	No	Yes	Yes	Yes	No	Yes	Yes Steganography, DCT
Implementation and Evaluation of Steganography Based Online Voting System	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes Steganography

Conclusion: -

A notable survey on voting systems, alongside visual cryptography techniques, has been considered to obtain an appropriate assessment of advancements in the sector. The advancement towards the VC is substantial; yet, each author delineates a distinct type and methodology for establishing an effective online voting system. I believe that a straightforward and successful approach should be implemented, and future research phases might include a comparison analysis of success and failure rates that can be quantified. This is a comprehensive study conducted in relation to several publications, papers, and special editions concerning the topic of online voting and the concept of VC.

References: -

1. Archana, P. S., & Ambily, O. (2016). Visual cryptography in internet voting for extended security. International Journal of Engineering Research and General Science, 4(2), 365–368.

2. Fisher, K., Carback, R., & Sherman, A. T. (2006). Punchscan : Introduction and System Definition of a High- Integrity Election System. Direct.
3. Hutchison, D., & Mitchell, J. C. (1973). Lecture Notes in Computer Science. Lecture Notes in Computer Science (Vol. 9). https://doi.org/10.1016/0020-7101(78)90038-7
4. Jadhav, P., Pawar, M., Ahire, P., Kumar, V., & Kulkarni, P. J. B. (2015). Online Polling System Using Extended Visual Cryptography, 4(6), 12340–12344.
5. Jaya, Malik, S., Aggarwal, A., & Sardana, A. (2011). Novel authentication system using visual cryptography. Proceedings of the 2011 World Congress on Information and Communication Technologies, WICT 2011, 1181–1186. https://doi.org/10.1109/WICT.2011.6141416
6. Kamdi, A., Kamble, M., Tayade, V., & Rajeev, N. (2017). A NOVEL APPROACH FOR ONLINE VOTING SYSTEM USING, (4), 63–66.
7. Kate, N., & Katti, J. V. (2017). Security of Remote voting system based on visual cryptography and SHA. Proceedings - 2nd International Conference on Computing, Communication, Control and Automation, ICCUBEA 2016. https://doi.org/10.1109/ICCUBEA.2016.7860071
8. Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system. Proceedings - IEEE Symposium on Security and Privacy, 2004(May), 27–40. https://doi.org/10.1109/SECPRI.2004.1301313
9. Mikail, O., Oladiran Tayo, A., Elijah Olusayo, O., & Oladotun Olusola, O. (2013). A Survey of Cryptographic and Stegano-Cryptographic Models for Secure Electronic Voting System. Covenant Journal of Informatics and Communication Technology (CJICT), 1(2), 54–78.
10. Nelli, R. R., Mehra, R., Madri, P., S, M., & J, R. (2017). Anti-Phishing I-Voting System using Visual Cryptography. Ijarcce, 6(5), 113–119. https://doi.org/10.17148/ijarcce.2017.6522
11. Patidar, P. K., Kushwah, R., & Chaudhari, T. (2017). and Face Detection- A Survey, 5(Ix), 633–635.
12. Rahul, H., Ghorpade, P., Shivaji, V., Renuka, P., Choudhari, A., & M, P. P. J. A. (2016). Internet Voting System using Visual Cryptography, 4(02), 2022–2024.
13. Rajendra, A. B., & Sheshadri, H. S. (2013). Visual cryptography in internet voting system. 2013 3rd International Conference on Innovative Computing Technology, INTECH 2013, 60–64. https://doi.org/10.1109/INTECH.2013.6653684
14. Raviraja Holla, M., & Suma, D. (2019). Pipelined parallel rotational visual cryptography (PPRVC). Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing, ICCSP 2019, 109–113. https://doi.org/10.1109/ICCSP.2019.8697957
15. Rura, L., Issac, B., & Haldar, M. K. (2017). Online voting system based on image steganography and visual cryptography. Journal of Computing and Information Technology, 25(1), 47–61. https://doi.org/10.20532/cit.2017.1003224
16. Rura, L., Issac, B., & Haldar, M. K. (2011). Online voting verification with cryptography and steganography approaches. Proceedings of 2011 International Conference on Computer Science and Network Technology, ICCSNT 2011, 1, 125–129. https://doi.org/10.1109/ICCSNT.2011.6181923
17. Rura, L., Issac, B., & Haldar, M. K. (2016). Implementation and evaluation of steganography based online voting system. International Journal of Electronic Government Research, 12(3), 71–93. https://doi.org/10.4018/IJEGR.2016070105