WALAILAK JOURNAL
Applied Sciences
http://wjst.wu.ac.th https://doi.org/10.48048/wjst.2021.8972

Secure Online Voting System using Visual Cryptography

Meher Gayatri Devi TIWARI[*] and Anil Kumar KAKELLI

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India

([*]Corresponding author's e-mail: mehergayatri17@gmail.com)

Received: 24 September 2019, Revised: 22 May 2021, Accepted: 29 May 2021

Abstract

The development of a secure online voting system using visual cryptography is highly essential for present voting systems. Based on the current requirements and design aspects of an existing online voting system, emerging technologies are required in online voting schemes, and these are examined in this work. The emerging cryptographic techniques which are suitable for secure online voting systems are analyzed. Techniques like password hashed-based schemes, visual cryptography, and threshold decryption cryptosystem are highlighted for secure online voting systems. Visual cryptography (VC) is a technique where visual information can be encrypted on the user side, with the information decrypted on the admin side, which can be helpful in allowing participation in voting systems securely and ensuring fast vote counting and monitoring of the voting process to achieve high accuracy while being scam-free. The proposed secure online voting system using visual cryptography is efficiently developed using Python and achieves better performance on minimum software and hardware configuration systems.

Keywords: Visual Cryptography, E-voting, Security, Techniques, Performance

Introduction

Visual cryptography (VC) is a technique where visual information, such as texts, pictures, videos, etc., can be encrypted efficiently, with the decryption of the information being as a visual image. Visual secret-keeping is a scheme that securely shares a system [1,2]. It splits the data and shares it, rather than encrypting it and saving it in a single place. Hence, there are several ways for securing the data, such as storing it in two places by splitting it into two shares or "n" shares. Most of the existing research work has used two secret shares, where one is provided to the voter using email or the computer being logged in, and the other is stored in the database of the voting system. This helps the system be transparent and also allows the system to run efficiently [3,4]. There is no ciphertext, as the shares act as the same. VC is the expansion of the requirement with limited memory. It is completely secure and increases the efficiency of working, as it involves a regulatory structure. VC can be used for a variety of systems and applications [5], which shows a greater evolution and has larger impact on growth.

E-voting is a process of voting using the internet or an electronic way for the easy casting of votes, accurate counting of the votes, and monitoring; it is professional and is also scam-free. This system stores the data on a computer system to make the voting system be faster and have also flawless counting [6]. Existing voting systems can allow multiple casting of votes and, hence, the process is enumerated as online voting and as better e-voting. The existing e-voting systems have the mechanism of VC. Some of the other techniques, like steganography, where encryption algorithms are combined with VC, have been used for better security [7]. The evaluation of the system needs to be very particular and, hence, a few more techniques and the involvement of admin are included to avoid natural forgery. This type of system can be used in both lower and higher forums of elections. People away from their native places can also vote with the accuracy of an authorized person, who has to be elected for the particular position [8]. As a result of the enumeration towards the system, the researchers and the developers who designing a system

should focus on security with high priority, as well as ensuring the system is user-friendly, with high performance, cost-efficiency, speed, and usability.

Literature survey

Comparative analysis of the various online voting systems: Objectives, techniques, and algorithms (**Table 1**).

Table 1 Comparative analysis of the various online voting systems: Objectives, techniques, and algorithms.

Title	Proposed Method	Objective	Techniques/ Algorithms used	Result
Remote voting system- for corporate companies using visual cryptography	This paper aims to allow the casting of votes while the confidential and critical conditions of corporate decisions are addressed in a very efficient way. This particular method makes it so flexible that it allows casting of votes from any remote place, and during times when key stakeholders of the election process are unavailable in the workplace.	Voting via the internet, keeping track of the system, designing proper security goals, maintaining transparency while compared to the present work, making the work a success [9], and bringing over accurate results.	From the lowercase letters and also the numbers available, 12 characters are selected randomly and encoded with a 64-bit key. SSL certification [10] is asked for, to be checked by the users by sending them a valid Ki value by the election server. This kind of protocol is flexible and capable of serving to both authenticate the voter with the election server and vice versa.	From the result of this work, a voting system should be based on security measures and also on the accuracy of voting. The system should be tested to make sure that it provides the process with reliability and intuitive indications for the voter.
Developing a visual cryptography tool for Arabic text	This paper involves Arabic language exposure towards the VC technique. According to the author, there are many studies have researched VC, but Arabic has not been focused on; Arabic nowadays holds a lot of importance, and in many places the language is used [4]. Henceforth, the author puts VC techniques towards it. The tool designed can be similarly followed for electronic voting, anti-phishing, Captcha, watermarking, biometric privacy, online payment systems, and digital signature in the Arabic environment.	Arabic is written from right to left, unlike English which is written from left to right. The Arabic letters look complicated as they seem to be attached when written or printed. The study concludes that a lot of techniques have been developed to identify and keep data safe and legible, as there are many Arabic-speaking internet users.	The size of the image is set in canvas as a function. The location is drawn and the background color is set to be white. Later, a *createTextImage()* [11] function is used for the text to be embedded and created in Arabic text. The position for the image is chosen randomly as the text is written. The limitation of the relatively small number of participants is considered.	The work shows the average time and effectiveness that is recognized in the text and the satisfaction with it. The tool is also advanced and is capable of being helpful in practical security appliances like Arabic CAPTCHAs [12]. This way, the study is also an enhanced method of understanding the language, which is growing efficient with its usability.
A novel approach for online voting system using visual	This paper discusses the advantages, disadvantages, and comparison of a few	It is helpful for people to vote from anywhere, as they need not wait in	A person need not go anywhere; they can stay home and cast a vote. This	As a result, it is easy for voters to vote via the internet. Counting

Title	Proposed Method	Objective	Techniques/ Algorithms used	Result
cryptography and face detection	e-voting systems. It also proposes a system that overcomes a drawback where VC can be introduced along with face detection, as it can provides a more suitable way of voting, is user friendly, and has more security.	queues, and also allows them not to bring an instinct if not voting because of work, as it makes an urge to a person making lethargic. To get a full number of votes. The system involves face detection [14] and VC as the algorithm technique.	makes it easy to allow the maximum amount of votes to be collected. Hence, it is convenient in whichever way the vote can be cast [13]. E-voting becomes secure with some safe algorithms being used and ensures people cast votes only once. Areas involved include providing security, avoiding phishing attackers, and also decreasing bogus voting.	the vote becomes very easy. Registration brings in voter and provides ID through which the process can be done and can allow the voting to be done in a very efficient way. Admin permissions are different from the user, where the admin can only view the results. Fake or incorrect details do not allow citizens to register for e-vote.
Visual cryptography in internet voting for extended security	This paper aims for e-voting as it makes the process automatic and easy to vote from anywhere across the limits of voting. VC and steganography are used to keep secrecy in advance. A secret password is enabled inside one image, which is split in two parts, where both are shared at once by the user to allow voting without invasion. This system becomes user-friendly as it is safe and admin permissions are separate from the users. It allows the casting of votes from any location without any problems.	Elections happen in both large- and small-scale ways, as it helps in appointing the right person without any partiality [15]. Since elections are restricted towards a location or area, e-voting removes the barrier of inconvenience. This is being done with VC, along with sufficient security.	1. User registers. 2. Admin checks and views with ID proof. 3. Validity to vote is accepted; otherwise rejected. 4. User login with credentials allows the downloading of a security image. 5. User sends email ID and upload both the shares. 6. Admin rechecks if it matches with the VC. 7. User votes only once and cannot vote again even if any mistake is made. 8. User logs out automatically and can view the result only once it is published.	As a result of this work, the design is being used in many large forums of voting. This particular system uses a 2-way client-server authentication process [16] which provides more security. Using this system, people can cast votes from wherever they are. The VC technique used allows decryption visually, as it becomes easier for the user. It becomes more secure.
Online polling system using extended visual cryptography	This paper offers benefits such as cost efficiency and increase of voters. In simple terms, it allows people to vote from wherever they are, irrespective of their location, along with security. The VC technique gives rise to a more secure way of online polling, and considers human factors in a careful way.	It becomes very flexible for the vote to be cast from any remote place, even when voters are unavailable for the process. This kind of feature is provided by VC [17]. It also takes care of human factors and also the security measures of voting.	It shares the secret image in a registration phase as a part of creating security within a server [18]. Here, the technique of VC is used as a security scheme. This scheme allows the giving of credentials to a user, which is accepted by the server only if the correct ones are entered for participation in voting.	As a result of this work, the government is spending a lot of money on the election; apart from this it is now known that the voting percentage is less and there is a chance to stop fraud [19]. The percentage of voting can be increased; also, the amount spent can be reduced.
Online voting system using visual cryptography and face	The work compares the existing e-voting systems, their drawbacks, and also	Some of the misleading effects in the present methods are privacy-	Fingerprinting as a way of voting has become an automated way of personal	As a result of this work, the sharing of some prominent technologies

Title	Proposed Method	Objective	Techniques/ Algorithms used	Result
detection- a survey	their advantages. It proposes a mechanism where VC along with face detection is collaboratively used. This provides more efficiency, appropriate voting, and a user-friendly and secure mechanism.	breach and fake votes, resulting in distortion and disturbance in an election and ballot snatching [20]. The work is effective and efficient, and enumerates the system as estimated.	identification which allows verification and also security. Rather than this, face detection using VC is used to make it easier and more feasible to vote from anywhere [21]. The secret sharing scheme does not allow any information to be exposed.	can solve the voting methods. The efficient mechanism of VC reduces the efforts and also makes the system run smoothly. It also provides security and mutual authentication for the client and server involved.
Anti-phishing I-voting system using visual cryptography	This paper aims for voting to be easy from remote places. A user can cast vote using credentials with security. A password is generated using a VC technique. The election committee sends two secret keys, one user and one system. Both are matched and then a vote can be cast. This is from the VC technique. It is supposed to be secure and has to be kept away from anyone; otherwise, it will not be accepted. Phishing involves attempting to get personal information in any possible way. It mostly happens by email or spoofing by users whose information can be used in a fake website.	Network security has been growing on a larger scale [22]. It is used for accessing data with a secure platform where the admin rights are given with proper credentials. Phishing is the stealing of private and sensitive information for malicious reasons. The data stolen by phishing can be used in any forum in a fake format.	A method is proposed to prevent and detect phishing. It is based on Anti-phishing Image Captcha using the VC technique [23]. Only authorized people will be allowed to vote where it prevents phishing. The server picks a text image as a password for registration, which is the same as used for login. Then, the secret key should be shared. Hence, the username and captcha can be generated, and phishing can be prevented as per the authentication being done. Verification is made, which has to be prominent for anti-phishing.	As a result of the paper, the VC technique is used to prevent phishing. Once done, it can be used in many large- and small-scale places. This safely allows the casting of votes so as to be utilized in all the places for casting votes. The voter can cast only once and cannot redo it. The phishing website does not display an image if it is real [24]. An intruder is not allowed to enter the website even by knowing the credentials.
Internet voting system using Visual Cryptography	This paper helps in more security using the VC technique, also using a secure password. "ONLINE VOTING SYSTEM" is the latest technology. It makes it easy to vote from anywhere. All the data is stored in a server with high security.	E-voting becomes easier and also involves more people [25]. It makes it user-friendly and particular in providing the voters with reliability. It is proposed with the VC technique.	It is proposed that this system will be used in many lower and higher places for voting as it is cost-efficient and uses time management. It has a client-server system [26]. Both the admin and the user have different rights as required. Data is stored and removed within the stipulated time.	As a result, this system can be used in a company's election or in government voting; it will be very easy for all citizens to vote in e-voting method from anywhere they are as it becomes secure by using the VC technique [27].
Novel authentication system using Visual Cryptography	This paper aims to compare the VC technique with some of its methods like pixel expansion, number of shares, size, quality of reconstructed image, etc. It improves cost-efficiency, along with	Security is taken care of, where nothing can be faked. This technique can also be used in safe systems for debit cards. This system helps in protecting fraud of the card [29].	This full method is similar to handling by the CA (Chartered Accountant) and the bank. Every authorization is given through the CA and the bank accepts the authorization, then each	A result of this system brings in the VC technique of color, which was proposed to have more security towards the system to prevent forgery. This can be put into systems

Title	Proposed Method	Objective	Techniques/ Algorithms used	Result
	the level of security it upholds.		request made by the bank is confirmed by the CA from the customer and processed for verification [28].	such as credit/ debit cards, and also voting.
E-voting system using visual cryptography secure multi-party computation	This paper aims for identification proofs to be monitored so that any fakes can be prevented and cross-checked to deny the approval. A multi-party system is used to keep the system secure, and also allows it to be reliable and transparent. It also monitors so that a person is only allowed to vote once. The four phases of the system used are: 1. The voter's enrolment, 2. Voter's authentication, 3. Vote casting and recording, and 4. Vote counting and election result publication.	It provides a model for time complexity and smoothness of voting, as it helps voting to be done from anywhere [30]. Security is also kept as the highest priority. The system uses the VC technique and biometrics to allow authentication to be kept in a very relevant and structured way.	The process is about constructing and reconstructing biometrics, as each example is unique; there are two parts. One part is stored in the voter's ID card, and the other is in the database; hence, both will be activated only if it is done live to prevent forgery [31]. Also, the algorithm that is used does not allow reconstruction if there is only one part available. Here, security plays a very important role.	As a result of the system that is used, it is known that two ways of authentication make the votes and the voters secure and prevent falsification. It improves the system by involving the data being stored in multiple places rather than putting it in one place, which makes it easy for it to be traced. Hence, this is one of the recent and the most effective systems.
Visual cryptography in internet voting system	This paper brings in a system which involves the technique of VC into the internet voting system (IVC). It helps in voting from anywhere, and also focuses on the security measures that are taken for the system to stay confidential. Only the correct credentials will allow the user to use the portal. A password is generated by two2 merge shares (Black and White share) from the VC technique.	The system provides two shared secrets, where one is given to the voter and one is in the database that is launched [32]. Hence, the voter has to log in with the right credentials and get into the system to vote. It is kept securely so that forgery and falsification can be eliminated from the system.	The VC technique used to implement high security in the system is a 2 to 2 sharing system, as there are many more sharing techniques. Here, even if one part of the secret key is present, cracking the system is not allowed unless the other is present. This is one of the most secure mechanisms for storing and obtaining a vote from an enrolled citizen [33]. The VC technique is used to authenticate the right one.	The method and the systems used in this project allow a person to vote from anywhere without any disturbance or inconvenience. The system is secure and cross-checks identification proofs so that the user does not falsify ID. Time complexity and cost efficiency have also been considered as a matter of fact.
Online voting verification with cryptography and steganography approaches	This is a system of e-voting with VC and steganography techniques. Users enroll and learn about the process step by step; nothing will be hidden or be flawed. The system makes the process secure and it is also cost and time-efficient. It allows a person to vote	The system has 3 main processes that are undergone in the system [34]. The steps are registration and authentication, tallying, and verification of vote. Eligibility is checked with the email ID and forgery is denied.	An E2E (end-to-end) voting system is constructed with the help of the image steganography technique of DCT co-efficient, which is efficient than the other techniques that are available for data hiding [35]. This kind of security is highly secure and makes	As a result of the system, a lot of vulnerabilities have been overcome. It helps in cost efficiency and also in faster performance. Some benefits are trustworthiness, reduction of other hardware use, particular

Title	Proposed Method	Objective	Techniques/ Algorithms used	Result
	from any place of limits.		it very difficult for a forger to find original data. This way, data is stored in multiple fragments and places with VC and is also kept encrypted.	device procurement, installation, upgrades, and maintenance, which allow the system to be secure.
Implementation and evaluation of steganography-based online voting system	This paper is one of the most recent and best; it involves many techniques, such as E2E steganography and VC for security. The encryption is hash-based and decryption is threshold-based. Performance and usability are improved. A voter can vote from any place as the limits will also be featured as per the officials.	This is a type of client-server process where the vote can only be cast once, and only by the registered user, as there will be verification [36]. On the other hand, the server is left up to the trustworthy environment to be liable to the system.	The method uses image steganography and VC is more secure, with forgery impossible. Three factors of monitoring are included- voter, polling officer, and system admin. The system of security here is different; in normal cryptography a ciphertext is given, but here, a stegno-object [37] is released, which is more secure.	Firstly, this system was put into a drill, and then a survey was taken and then implemented. Secondly, the system has two shared secrets which are not kept in one place; one with a user and the other in the server. Hence, the system cannot be easily fooled. This makes the system user-friendly, secure, high performing, cost and time-efficient, and also easily usable.

Proposed algorithm

Table 2 explains the algorithm used to acquire the connection of server and client. As per the algorithm, after successful connection establishment between the server and client [38], the required information is gathered from a user through a few questionnaires, as per the protocol of user registration. Thereafter, a visual image will be sent to the user for the next level of the process, as mentioned in the next algorithm.

Table 2 Proposed secure online voting system using VC.

Algorithm:

1. *Start*
2. *Image encryption*
3. *Input ← hidden Image.*
4. *Output → Encrypted Image.*
5. *Choose input RGB image*
   Separate R-G-B Channels
6. *Each channel encrypted → receive 8 shares using key (Ki)*
7. *From step 5, result 24 shares*
8. *8 shares of each channel compress to 3 shares.*
9. *Output: encrypted image*
10. *End*

Table 3 denotes and shows the usage of the cryptographic algorithm for verifying the user credentials and authorizing and authenticating the person to cast a vote. Hence, the image is sent to the credentials given once approved. This later also allows for voting [39].

Table 3 Proposed cryptographic algorithm for user authorization.

Algorithm:

1. *Start*
2. *Send a cryptographic image to finish registration*
3. *Choose a random radiant*
4. *generates image of 97,122 measure*
5. *Image⟶ QR code*
6. *Image shares merged if image of the database is released*
7. *Image merge⟶ generate new unique Captcha code (nuCc)*
8. *Use nuCc (relevant password) for login or cast the vote.*
9. *Verify the database*
10. *End*

```
img = Image.new('1', (150, 150), color=255)  # creates a new image sized 150x150, black&white (mode 1)
self.txt = ''
for i in range(6):
    self.txt += chr(random.randint(97, 122))
ImageDraw.Draw(img).text(xy=(0, 50), text=self.txt,
                         font=ImageFont.truetype('C:\WINDOWS\Fonts\ARLRDBD.TTF'
                         , 37))
```

Figure 1 Syntax used in Visual Cryptography (VC).

Working modules and methodology of the proposed system

Module 1: Initialize the server

The high commission involves the nominees or the name of the parties, submits them to the host, and acquires votes for them. After the submission, the sever system will be initiated and be ready for the client systems, as shown in **Figure 2**.

```
    if (server_socket != None):
        server_socket.close()
    sys.exit()


def main():
    try:
        after_func1()
    except:
        sys.exit()


if __name__ == '__main__':
    main()
```

```
Server started!
Waiting for clients...
```

Figure 2 Server initialization module for the clients.

Module 2: Shares of password

Some mandatory data, along with email IDs, are required from the user/client for user authorization. The secure key share will be sent to the registered user email ID, and another share is stored in the database, as shown in **Figure 3**.

Figure 3 One share password sent to registered client email ID.

Module 3: Authentication

Once the password is cross-referenced by a server, it provides a source image which has to be entered in the place instead of a code. Hence, the person is authenticated to vote, as shown in **Figure 4**.

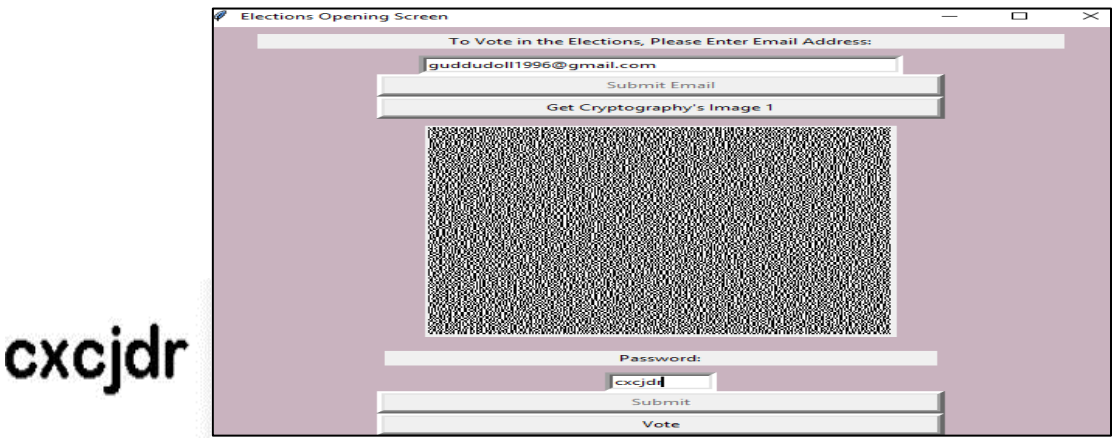

Figure 4 Captcha code password after the merging of 2 codes.

Module 4: Casting the Vote

Once the person is authenticated with the fulfillment of necessary security norms, the system leads to the voting page for one-time-only voting. There is no chance for forgery, due to double encryption, as shown in **Figure 5**.

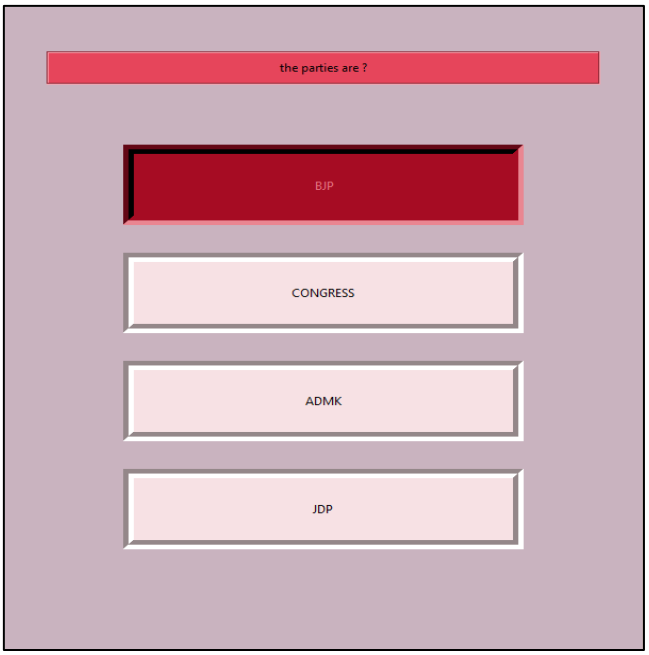

Figure 5 Casting of vote to a desired party.

Module 5: Result analysis

This module can be monitored on the server end to allow the counting of votes in a faster manner, and also prevents conspiracy, because the server is initiated first, which is liable to access the results, as shown in **Figure 6**.

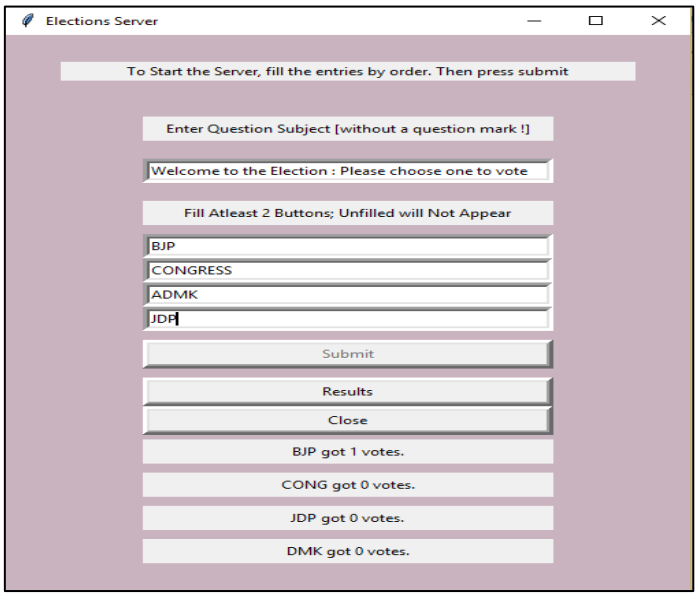

Figure 6 Result analysis from server end.

Proposed system implementation

The proposed system is a combination of four major components: server, client, database, and cryptography technique. The server is handled by the local government to enable the various political parties to participate in the election. The database is a mutual platform that is handled on the server end to declare the results to the client. The client platform possesses cryptography [40] which is described in the proposed algorithm, **Table 3**, for secure voting. The voter undergoes the process of the secure methods initiated by the proposed system for voting on the chosen dates. This work has been implemented based on visual cryptography to help the voting system to be efficient. Our proposed voting system is highly secure and results in better performance, speed, and user-friendliness as compared to the existing systems, as shown in **Figure 7**. The other requirements, based on geographical conditions, user authentication, and authorization [41], can be modified as per the need of the admin. Hence, the below **Figure 9** shows the link between and the connectivity of the 4 main factors involved.

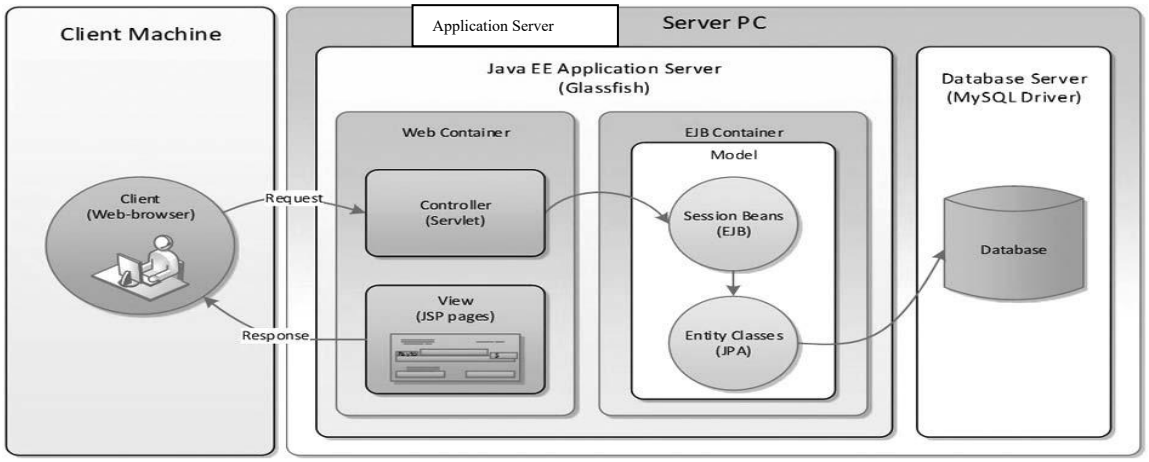

Figure 9 Implementation model.

The role of server

1. The teams or the parties involved in the voting system are stored.
2. The votes are collected and linked to the database.
3. A connection is established between the client and the database [42]
4. Python code is activated, which helps in the padding.
5. The secure online voting system is developed using Python efficiently, using Jupyter and SQLite3 database server with Anaconda application.
6. Localhost server is used as the back end, and the front end is managed by a hypertext markup language.
7. The processes of the voting system are initialized, activated, monitored, and stored.

The role of client

1. Server connection establishment.
2. Used by voters to vote for the desired party.
3. One-time voting system.
4. Secure connection between the client and server.
5. User authentication [43].
6. Storage of the casted votes by the client in this connection.
7. Password verification and authorization.

The role of database

1. A table is created where the email text and the vote text are accommodated and accumulated.
2. The email and the votes are inserted into the votes as the registration is made.
3. Results are also stored in the database for display [44].
4. Verification of the mail and the data is provided by the user.
5. The session is initiated and terminated [45,46].

Graph

Performance, speed, user-friendliness, and security are the major concerns of the proposed work and are presented in **Figure 10** using various test cases which have been passed by time consistency. The below graph is formulated with various performance parameters from the research work mentioned in the literature survey section. Hereby, these points are given completely with the comparison of the existing work and compared with the proposed work. The proposed work has been developed using Python, JavaScript, and HTML coding, and tested with various performance parameters and test cases of 20 different samples.

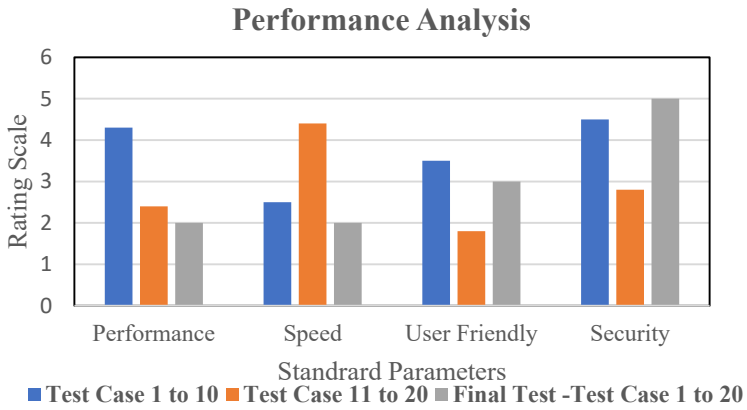

Figure 10 Performance analysis of the proposed secure online voting system with various test cases.

Conclusions

The proposed system is implemented using visual cryptography for security, efficiency, simplicity, and ease of use to allow all categories of user to cast votes. We have developed a prototype for the proposed system, tested it using various test cases, and analyzed the system performance in a real-time environment. The population living across the globe is increasing and cannot utilize voting opportunities due to busy work schedules, are unable to travel long distances, or have social security issues. The proposed system is novel and successful in overcoming all these limitations of the voters in casting their votes in a secure manner, irrespective of location, gender, social status, or personal issues. For the future, we are upgrading our work so that it can be easily configurable for all platforms and can easily modify the roles and responsibilities as per the user/admin requirements, using a lightweight authentication mechanism which can fulfill the rules and regulations of the local government with internal security and safety measures. Hence, this is a profound work done positively with no false claims made for our system.

References

[1] SA Alsuhibany. Developing a visual cryptography tool for Arabic text. *IEEE Access* 2019; **7**, 76573-9.
[2] PS Archana and O Ambily. Visual cryptography in internet voting for extended security. *Int. J. Eng. Res. Gen. Sci.* 2016; **4**, 365-8.
[3] AG Bhosale and VS Patil. A (2, 2) visual cryptography technique with improved contrast. *Inform. Secur. J. Global Perspective* 2020; **29**, 199-208.
[4] T Chakraborty, S Ghosh, T Ghosh, C Mizan and S Karmakar. (3, 3) Visual cryptography for online certificate authentication. *Int. J. Eng. Adv. Tech.* 2020; **9**, 152-6.
[5] IDC Challener. United States patent. *Geothermics* 1985; **14**, 595-9.
[6] NM Chayal and NP Patel. *Review of machine learning and data mining methods to predict different cyberattacks. In*: K Kotecha, V Piuri, H Shah and R Patel (Eds.). Data science and intelligent applications. Lecture notes on data engineering and communications technologies. Springer, Singapore, 2021, p. 43-51.
[7] PL Chiu and KH Lee. Threshold visual cryptography schemes with tagged shares. *IEEE Access* 2020; **8**, 111330-46.
[8] K Fisher, R Carback and AT Sherman. Punchscan: Introduction and system definition of a high-integrity election system. *In*: Proceedings of the 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK. 2006.
[9] Y Guo, X Jia, Q Chu and D Wang. A novel XOR-based threshold visual cryptography with adjustable pixel expansion. *Appl. Sci.* 2020; **10**, 1321.
[10] K Gurunathan and SP Rajagopalan. A stegano - visual cryptography technique for multimedia security. *Multimed. Tool. Appl.* 2020; **79**, 3893-911.
[11] D Hutchison and JC Mitchell. Lecture notes in computer science. Vol. 15-L-systems: Edited by G. Goos and J. Hartmanis. Springer Verlag, Berlin, 1976. vi + 338 pp. *Lecture Notes Comput. Sci.* 1978; **9**, 242.
[12] DR Ibrahim, JS The and R Abdullah. Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization. *Inform. Secur. J. Global Perspective* 2021; **30**, 149-59.
[13] P Jadhav, M Pawar, P Ahire, V Kumar and PJB Kulkarni. Online polling system using extended visual cryptography. *Int. J. Eng. Comput. Sci.* 2015; **4**, 12340-4.
[14] B Jagadeesh and KLSP Reddy. Image security using digital image watermarking and visual cryptography techniques. *Int. J. Innovat. Tech. Explor. Eng.* 2020; **9**, 2386-91.
[15] Jaya, S Malik, A Aggarwal and A Sardana. Novel authentication system using visual cryptography. *In*: Proceedings of the 2011 World Congress on Information and Communication Technologies, Mumbai, India. 2011, p. 1181-6.
[16] S Jiao, J Feng, Y Gao, T Lei and X Yuan. Visual cryptography in single-pixel imaging. *Optic. Express* 2019; **28**, 7301-13.
[17] GR Kadambi, PB Kumar and V Palade. *Lecture Notes in Electrical Engineering 649 Emerging Trends in Photonics, Signal Processing and Communication Engineering Proceedings of ICPSPCT 2018.* Springer, Singapore, 2020.
[18] A Kamdi, M Kamble, V Tayade, J Dharne and RN Verma. A novel approach for online voting system using visual cryptography and face detection. *Int. J. Adv. Electron. Comput. Sci.* 2017; **4**, 63-6.
[19] N Kate and JV Katti. Security of remote voting system based on visual cryptography and SHA. *In*: Proceedings of the 2nd International Conference on Computing, Communication, Control and Automation, Pune, India. 2016.
[20] T Kohno, A Stubblefield, AD Rubin and DS Wallach. Analysis of an electronic voting system. *In*: Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, California. 2004, p. 27-40.
[21] R Krimmer and M Volkamer. EVOTE2014. *In*: Proceedings of the 6th International Conference on Electronic Voting, Bregenz, Austria. 2014.

[22] P Li, J Ma and Q Ma. (t, k, n) XOR-based visual cryptography scheme with essential shadows. *J. Vis. Comm. Image Represent.* 2020; **72**, 102911.
[23] P Li, J Ma, L Yin and Q Ma. A construction method of (2, 3) visual cryptography scheme. *IEEE Access* 2020; **8**, 32840-9.
[24] P Li, L Yin and J Ma. Visual cryptography scheme with essential participants. *Mathematics* 2020; **8**, 838.
[25] A Makwe and AS Rathore. *An empirical study of neural network hyperparameters*. *In*: V Bhateja, SL Peng, SC Satapathy and YD Zhang (Eds.). Advances in intelligent systems and computing. Springer, Singapore, 2021.
[26] SH Masood and S Riza. Trends in selective laser sintering in biomedical engineering. *Int. J. Emerg. Trends Eng. Res.* 2020; **8**, 54-9.
[27] M Melkemi and K Hammoudi. Voronoi-based image representation applied to binary visual cryptography. *Signal Process. Image Comm.* 2020; **87**, 115913.
[28] OO Mikail, OT Arulogun, EO Omidiora and O Okediran. A survey of cryptographic and stegano-cryptographic models for secure electronic voting system. *Covenant J. Inform. Comm. Tech.* 2013; **1**, 54-78.
[29] MFM Mursi, GMR Assassa, A Abdelhafez and KAM Samra. On the development of electronic voting: A survey. *Int. J. Comput. Appl.* 2013; **61**, 1-11.
[30] PS Naidu, R Kharat, R Tekade, P Mendhe and V Magade. E-voting system using visual cryptography & secure multi-party computation. *In*: Proceedings of the 2nd International Conference on Computing, Communication, Control and Automation, Pune, India. 2016.
[31] RR Nelli, R Mehra, P Madri, S Monica and J Rajeshwari. Anti-phishing I-voting system using visual cryptography. *Int. J. Adv. Res. Comput. Comm. Eng.* 2017; **6**, 113-9.
[32] PK Patidar, R Kushwah and T Chaudhari. Online voting system using visual cryptography and face detection: A survey. *Int. J. Res. Appl. Sci. Eng. Tech.* 2017; **5**, 633-5.
[33] SD Purohit, DS Jat, RC Poonia, S Kumar and S Hiranwal. *In*: Proceedings of the International Conference on Communication and Computational Technologies. Springer, Singapore, 2021.
[34] HR Pralhad, GV Shivaji, PR Anil, CS Pritamchand and AM Jagtap. Internet voting system using visual cryptography. *Int. J. Sci. Res. Develop.* 2016; **4**, 2022-4.
[35] AB Rajendra and HS Sheshadri. Visual cryptography in internet voting system. *In*: Proceedings of the 3rd International Conference on Innovative Computing Technology, London, United Kingdom. 2013, p. 60-4.
[36] RM Holla and D Suma. Pipelined parallel rotational visual cryptography (PPRVC). *In*: Proceedings of the International Conference on Communication and Signal Processing, Chennai, India. 2019, p. 109-13.
[37] L Rura, B Issac and MK Haldar. Implementation and evaluation of steganography based online voting system. *Int. J. Electron. Govern. Res.* 2016; **12**, 71-93.
[38] L Rura, B Issac and MK Haldar. Online voting verification with cryptography and steganography approaches. *In*: Proceedings of International Conference on Computer Science and Network Technology, Harbin, China. 2011, p. 125-9.
[39] L Rura, B Issac and MK Haldar. Online voting system based on image steganography and visual cryptography. *J. Comput. Inform. Tech.* 2017; **25**, 47-61.
[40] MN Anusha and BK Srinivas. Remote voting system for corporate companies using visual cryptography. *Int. J. Adv. Res. Comput. Sci. Software Eng.* 2012; **2**, 250-4.
[41] GS Mary and SM Kumar. Secure grayscale image communication using significant visual cryptography scheme in real time applications. *Multimed. Tool. Appl*. 2020; **79**, 10363-82.
[42] SK Singh, M Yadav, A Chaudhary and U Singhal. Verifiable color progressive visual cryptography with cheating detection. *In*: Proceedings of the International Conference on Communication and Computational Technologies Algorithms for Intelligent Systems. Springer, Singapore, 2021, p. 535-45.
[43] J Tripathi, A Saini, Kishan, Nikhil and Shazad. Enhanced visual cryptography: An augmented model for image security. *Proc. Comput. Sci.* 2020; **167**, 323-33.

[44] X Wu and CN Yang. Probabilistic color visual cryptography schemes for black and white secret images. *J. Vis. Comm. Image Represent.* 2020; **70**, 102793.
[45] X Yan, F Liu, WQ Yan and Y Lu. Applying visual cryptography to enhance text captchas. *Mathematics* 2020; **8**, 332.
[46] T Zhao and Y Chi. Hierarchical visual cryptography for multisecret images based on a modified phase retrieval algorithm. *Multimed. Tool. Appl.* 2020; **79**, 12165-81.