iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.61482

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 12 Issue V May 2024- Available at www.ijraset.com

A Breakthrough Authentication Protocol for Fortifying IoT-Cloud Security

K.Subha[1], S. Hari Prasath[2], K. Kaarthik Roshan[3], M. Kalaimani[4]
[1]*Assistance Professor Computer Science And Engineering SRMIST RAMAPURAMCHENNAI*
[2, 3, 4]*B. Tech CSE with Specializationin Cyber Security, SRM University, India*

Abstract: ***Physical layer key generation, leveraging the reciprocity and randomness of wireless fading channels, has garnered significant research interest in recent years. While theoretical studies have demonstrated its potential to generate information-theoretically secure keys, challenges remain in translating theory into practice. This paper provides an overview of the physical layer key generation process and discusses its practical challenges. Various passive and active attacks are analyzed and evaluated through numerical studies. A new key generation scheme using random probing signals and combining user-generated randomness with channel randomness is introduced to counteract active attacks. Numerical results demonstrate that the proposed scheme achieves higher security strength than existing schemes using constant probing signals under active attacks. Secret-key generation relying on wireless channel reciprocity is an intriguing solution as it can be efficiently implemented at the physical layer of emerging wireless communication networks, while providing information-theoretic security guarantees. In this paper, we investigate and compare the secret-key capacity based on the sampling of the entire complex channel state information (CSI) or only its envelope, the received signal strength (RSS).***

I. INTRODUCTION

1) Current cryptographic approaches rely on the computational capabilities of non-legitimate terminals. As technology advances, ensuring the security of transmitted information becomes increasingly uncertain. In contrast, an information-theoretic approach provides a framework for future coding schemes that guarantee security independently of the computational capabilities of eavesdroppers. Wireless communications are vulnerable to eavesdropping due to their broadcasting nature. Traditional cryptography, with its high latency and unguaranteed secrecy, is less attractive for securing swift and highly mobile wireless communications. To address this, physical layer security (PLS) has been proposed, attracting considerable attention from both academia and industry. The core idea is to exploit the dynamics and random fading of wireless channels, avoiding the use of complex and high-latency cryptography techniques, thereby offering promising prospects for securing wireless communications.
2) With the proliferation of Internet of Things (IoT) devices, secure communication becomes essential. One common method to secure communication between wireless devices is to generate a symmetric key between them and use it for encryption and decryption. The Diffie-Hellman (D-H) key exchange protocol is a conventional mechanism for generating a shared secret key between two parties. However, the computational overhead of the D-H protocol, particularly the expensive exponential operations, is undesirable for resource-constrained devices such as embedded sensors, wearable devices, and RFIDs. Additionally, as attackers' computing power increases, the D-H protocol needs to increase the key length to maintain a certain level of security, exacerbating the computational overhead.
3) An alternative approach to generating a shared secret key between wireless devices is to exploit the reciprocity of the random fading channel. This mechanism, known as physical layer key generation, involves wireless devices measuring highly correlated wireless channel characteristics (e.g., channel impulse responses or received signal strengths) and using them as shared random sources to generate a shared key. In theory, in a rich multipath scattering environment, a passive attacker more than a half-wavelength away from the legitimate users will obtain uncorrelated channel measurements, thus unable to infer much information about the generated key.
4) As wireless communication requires the sharing of more information, authenticating devices and ensuring information security becomes a significant challenge. This challenge is particularly pronounced in IoT systems, where devices often have low computational capacity and power consumption. Therefore, it is necessary to reduce the cost of authentication and encryption while ensuring information security. By elaborating on these bounds, we aim to develop efficient and secure key generation schemes that can withstand eavesdropping attacks.

II. RELATED WORK

With the escalating number of threats in IoT cloud environments, the necessity for advanced security mechanisms to protect data against hacking and various cyber-attacks has become increasingly evident. Conventional cryptographic algorithms, while widely implemented, often fall short in providing adequate protection and can prove ineffective against evolving attack vectors [11]. In response to these challenges, researchers have explored alternative approaches, one of which involves visual cryptography-based authentication protocols. For instance, Smith et al. proposed a secure mutual authentication protocol based on visual cryptography. This protocol encrypts and decrypts secret images to authenticate users accessing cloud services [22]. To assess the security and effectiveness of such authentication protocols, researchers commonly employ the Barrows-Abadi-Needham (BAN) logic method. This method has been instrumental in evaluating the robustness of various authentication mechanisms, including those based on visual cryptography techniques [13].

Additionally, considerable research efforts have been directed towards the generation of secure keys for authentication. In this regard, Alice and Bob follow a series of steps, including channel probing, randomness extraction, quantization, information reconciliation, and privacy. In response to the increasing number of threats in IoT cloud environments, there has been a growing need for advanced security mechanisms to safeguard data against hacking and various cyber-attacks. Traditional cryptographic algorithms, while widely used, are often vulnerable to these attacks and can be inefficient against new attack vectors [11]. To address these limitations, researchers have explored alternative approaches, such as visual cryptography-based authentication protocols.

For instance, Smith et al. proposed a secure mutual authentication protocol based on visual cryptography, which encrypts and decrypts secret images to authenticate users accessing cloud services [12]. The security and effectiveness of such authentication protocols are often analyzed using the Barrows-Abadi-Needham (BAN) logic method, which has been shown to effectively assess the robustness of authentication mechanisms, including those based on visual cryptography techniques [23]. Additionally, research efforts have focused on the generation of secure keys for authentication, with Alice and Bob following a series of steps, including channel probing, randomness extraction, quantization, information reconciliation, and privacy amplification, to generate secure keys for communication amplification, to generate secure keys for communication [24].

III. PROPOSED METHOD

A. *Channel Probing*

Channel probing involves collecting channel measurements by Alice and Bob. These measurements include channel state information (CSI), received signal strength (RSS), or phase. During this step, Alice and Bob exchange channel probing signals. One channel probing consists of a pair of bi-directional channel probing with a short time lag, assuming a half-duplex radio..

B. *Randomness Extraction*

Utilizing feature-based classification techniques, the system extracts relevant features from textual content and user meta data. These features provide valuable insights into user behavior and interaction patterns, aiding in the identification of cyberbullying instances.

C. *Handling Negations*

To enhance the accuracy of cyberbullying detection, the system incorporates mechanisms to handle negations within text. By considering the context of negated statements, the system mitigates the risk of misclassification and improves the overall effectiveness of the detection process.

D. *Quantization*

Quantization techniques are employed to distill key insights from user-generated content. Quantization is the process of converting the extracted random channel measurements into bits.

E. *Information Reconciliation*

Information reconciliation is a form of error correction carried out between Alice and Bob to ensure that the keys generated separately on both sides are identical.

F. Collection of Channel Measurements

Alice and Bob collect channel state information (CSI), received signal strength (RSS), or phase measurements to characterize the wireless channel.

G. Deterministic Part Removal

Alice and Bob remove deterministic components from the received signals to extract randomness. The large-scale fluctuation pattern in the received signals, determined by the distance between Alice and Bob.

H. Security Risks

Certain bit information may be revealed to Eve during the reconciliation process, posing security risks. Imperfections in channel measurements due to imperfect reciprocity and the half-duplex property of the radio. Correction of errors between Alice and Bob to ensure the generated keys are identical. During the reconciliation process, parity bit information may be exchanged to correct errors, and a certain amount of bit information will be revealed to Eve.

I. Modeling Received Signals

The received signals are modeled as the transmitted sounding signal timing (in the frequency domain) channel gain plus noise. To ensure that the shared keys are not easily determined by attackers, Alice and Bob need to extract randomness caused by channel fading, thereby removing the large-scale component. A moving window average method can be used to extract small-scale randomness. This method has been instrumental in evaluating the robustness of various authentication mechanisms, including those based on visual cryptography techniques, additionally considerable research efforts have been directed towards the generation of secure keys for authentication. In this regard, Alice and Bob follow a series of steps, including channel probing, randomness extraction, quantization, information reconciliation, and privacy amplification, to generate secure keys for communication. However, broadcasting a key component is vulnerable to eavesdroppers if additional countermeasures are not taken. Moreover, various real-world tasks do not require individual information, and the superimposed signal is sufficient. Despite these limitations, the Barrows-Abadi-Needham logic was a significant advancement in the field of network security when it was introduced and has influenced the development of many subsequent authentication and key exchange protocols. Imperfections in channel measurements due to imperfect reciprocity and the half-duplex property of the radio.

IV. HARDWARE AND SOFTWARE REQUIREMENT

A. Backend Technologies:

1) Python: The system is built using the Python programming language, offering flexibility and a wide range of libraries for data analysis and machine learning.

2) NumPy: NumPy is utilized for numerical computing, providing efficient array operations and mathematical functions essential for data processing.

3) Sci-learn (scikit-learn): Sci-learn is a Python library used for machine learning tasks, including classification, regression, clustering, and model evaluation.

4) Jupyter Notebook: Jupyter Notebook serves as the interactive computing environment for developing and presenting the system's code and analysis. It enables seamless integration of code, visualizations, and explanatory text, facilitating reproducible research and collaboration.

B. Frontend Technologies:

C. Web Technologies:

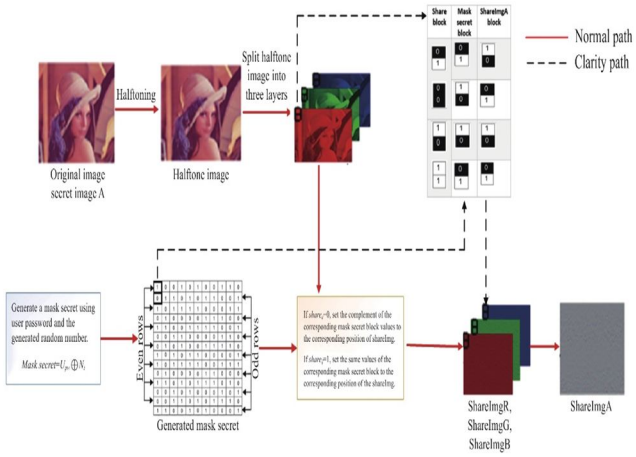
The frontend of the system utilizes web technologies for user interaction and visualization. The specific technologies employed may include:

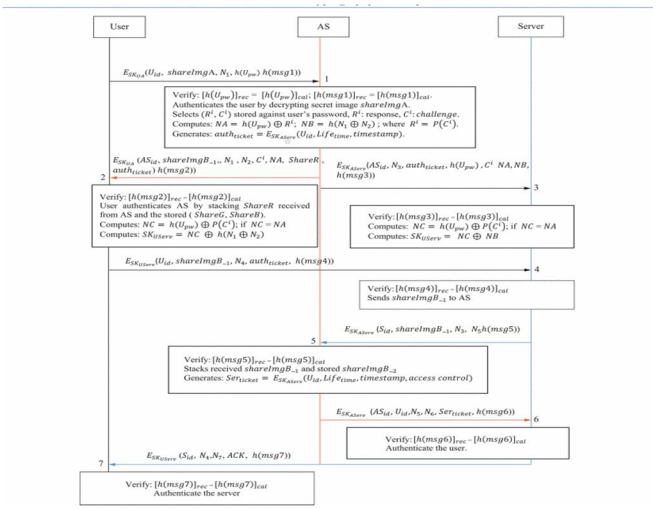
1) HTML: HTML is used for structuring the content of web pages, providing a standardized markup language for creating web interfaces.

2) CSS: CSS (Cascading Style Sheets) is used for styling web pages, allowing for customization of layout, colors, fonts, and other visual aspects.

3) JavaScript: JavaScript is employed for client-side scripting, enabling dynamic and interactive elements within web pages. Frameworks (e.g., React, Angular, Vue.js): Frontend frameworks may be used to facilitate the development of complex web applications, providing reusable components, state management, and routing capabilities.

V. ARCHITECTURE DIAGRAM





VI. PROPOSED ALGORITHM

A. Proposed Algorithm: Mean-Value Quantization Scheme

The proposed algorithm, Quantization is the first step of wireless key establishment, often employing thresholds to parse the sample values into binary bits based on certain channel metrics. Traditional quantization schemes use one or two thresholds to quantize samples to binary 0 or 1. In the basic threshold quantization scheme, only one threshold T When the sample value is larger than T, it is encoded as 1; otherwise the sample value is encoded as 0.

B. Advantages of Proposed Algorithm:

One of the key advantages of our system is its capability to perform multiple functions simultaneously. By leveraging advanced machine learning techniques, our system can handle various tasks concurrently, leading to increased efficiency and flexibility. This multifunctional capability allows our system to adapt to diverse requirements, making it suitable.

Another advantage of our system is its ability to learn from data to solve complex tasks. By utilizing data-driven learning algorithms, our system can analyze large datasets and extract valuable insights to improve its performance over time. This capability enables our system to adapt to changing environments and evolving security threats, ensuring robust and adaptive protection for data and user privacy in IoT cloud networks.

Additionally, our system has the capability to learn hidden relationships within the data without imposing any fixed relationships. Unlike traditional methods that rely on predefined rules and relationships, our system can autonomously discover patterns and correlations within the data, enabling more accurate and efficient decision-making.

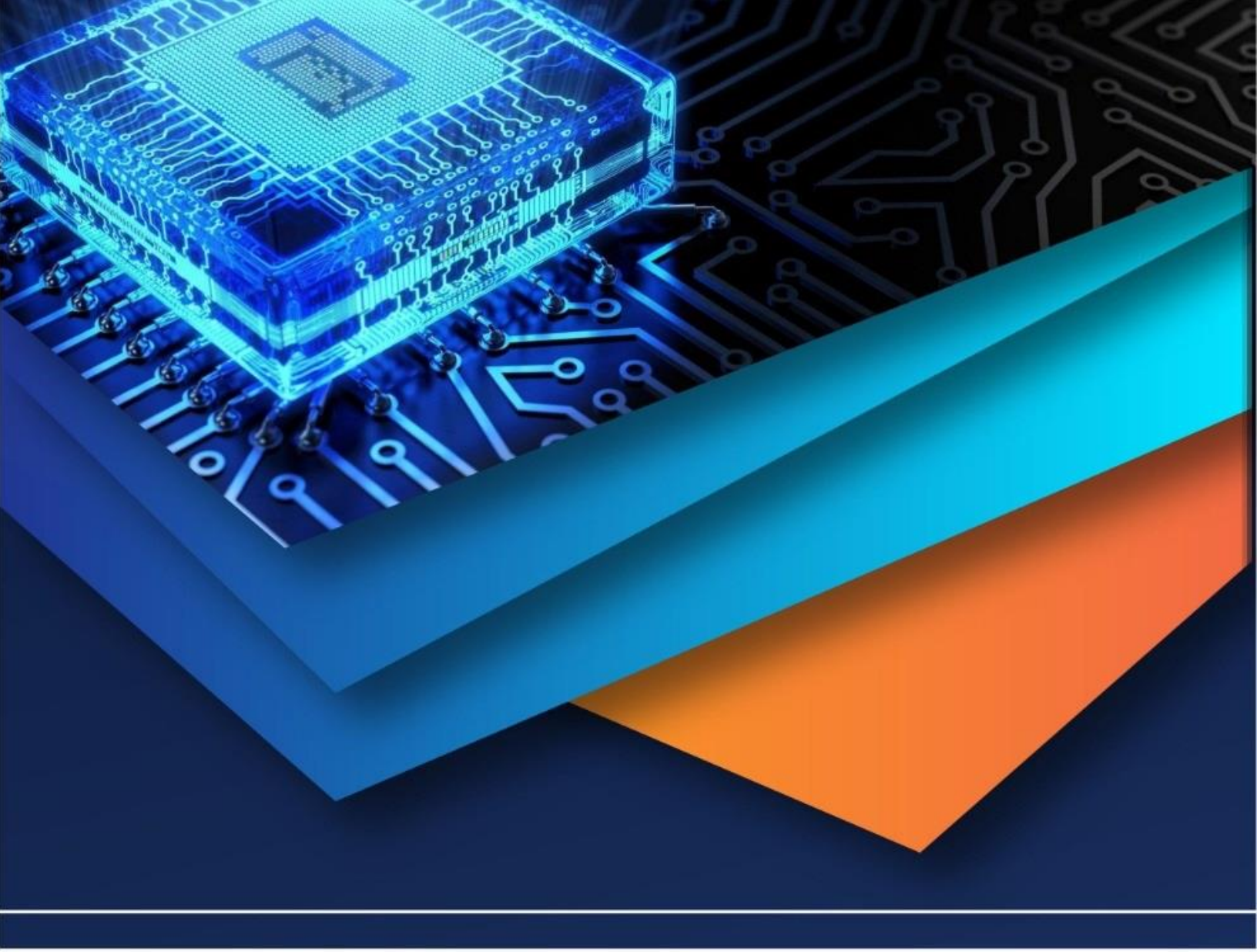
VII. CONCLUSION

In this work we have presented the concept of cyberbullying

The SK generation protocol which was introduced in this work used a two phase approach to achieve the given SK rate. In the first step, Alice estimated her state and sent this along with other information which was obtained from her observation to Bob. Although, this information is also received by Eve, it was shown that the strong secrecy and uniformity of the generated SK is still guaranteed. In the second step, Bob used this information including the estimated state of Alice to generate the SK. A single-letter lower-bound for the SK capacity of a finite compound source was derived as a function of the communication rate constraint between Alice and Bob. We model with proper pre-processing and post processing functions in order to match the with a function that outputs a secret key which includes information from other users. The model is also extended to multiple layers to obtain flexibility between the time and frequency resources. Lastly, we examine the performance of the proposed model for various scenarios in a competitive manner with the benchmark system. It is shown that the proposed model provides security against passive eavesdroppers in certain scenarios.

REFERENCES

[1] Brou Bernard Ehuil,Chen Chen,Shirui Wang,Hua Guo,Jianwei Liu,Ju Ren A Secure Mutual Authentication Protocol Based on Visual Cryptography Technique for IoT-Cloud Chinese Journal of Electronics, 2022
[2] Pei-Ling Chiu,Kai-Hui Lee Threshold Visual Cryptography Schemes With Tagged Shares IEEE Access, 2020
[3] Peng Li,Jianfeng Ma,Liping Yin,Quan Ma A Construction Method of (2, 3) Visual Cryptography Scheme IEEE Access, 2020
[4] Rui Sun,Zhengxin Fu,Bin Yu Size-Invariant Visual Cryptography With Improved Perceptual Quality for Grayscale
[5] Bhili Zhou,Ching-Nung Yang,Song-Ruei Cai,Dao-Shun Wang Boolean Operation Based Visual Cryptography IEEE Access, 2019
[6] T. Varinder, and P. Kanwar. "Understanding social media." Bookboon, 2012.
[7] Suliman A. Alsuhibany Developing a Visual Cryptography Tool for Arabic Text IEEE Access, 2019 M. Fishbein, and I. Ajzen. "Belief Attitude, Intention and to Theory and Research Introduction Behavior: A Reading."6, 1975.
[8] Yan Ke,Jia Liu,Min-Qing Zhang,Ting-Ting Su,Xiao-Yuan Yang Steganography Security: Principle and Practice IEEE 2020
[9] Rose Karen, Eldridge Scott and Chapin Lyman, The internet of things: An overview, The internet society (ISOC), vol. 80, pp. 1-50, 2015.
[10] R. Kalaiprasath, R. Elankavi and R. Udayakumar, Cloud security and compliance-a semantic approach in end to end security, International Journal on Smart Sensing and Intelligent Systems, vol. 10, no. 5, pp. 482-494, 2017.
[11] Hendre and K. P. Joshi, A semantic approach to cloud security and compliance, Proceedings of 2015 IEEE 8th International Conference on Cloud Computing, pp. 1081-1084, 2015.
[12] B. Rabiah, K. K. Ramakrishnan, E. Liri et al., A lightweight authentication and key exchange protocol for IoT, Proceedings of the Workshop on Decentralized IoT Security and Standards, pp. 1-6, 2018.
[13] M. Naor and A. Shamir, Visual cryptography in Advances in Cryptology-EUROCRYPT, Berlin, Germany:Springer, vol. 950, pp. 1-12, 1995.
[14] H. Koga and E. Ueda, Basic properties of the (t n)-threshold visual secret sharing scheme with perfect reconstruction of black pixels, Des. Codes Cryptogr., vol. 40, no. 1, pp. 81-102, Jul. 2006.
[15] J. Weir and W. Q. Yan, Visual Cryptography and Its Applications, Frederiksberg, Denmark:Ventus Publishing
[16] J. Weir and W. Q. Yan, Visual Cryptography and Its Applications, Frederiksberg, Denmark:Ventus Publishing pp. 165496-165508, 2019.
[17] M. Naor and A. Shamir, Visual cryptography, Proc. Workshop Theory Appl. Cryptogr. Techn. (EUROCRYPT), pp. 1-12, 1994.
[18] S. Droste, New results on visual cryptography in Advances in Cryptologyâ€"CRYPTOâ€™96, Berlin,
[19] C. Blundo, S. Cimato and A. De Santis, Visual cryptography schemes with optimal pixel expansion, Theor. Comput. Sci., vol. 369, no. 1, pp. 169-182, Dec. 2006.
[20] F. Liu, C. Wu and X. Lin, Step construction of visual cryptography schemes, IEEE Trans. Inf. Forensics Security.
[21] R. Lakshmanan and S. Arumugam, Construction of a (k n)-visual cryptography scheme, Des. Codes Cryptogr. vol. 82, no. 3, pp. 629-645, Mar. 2017.
[22] M. Naor and A. Shamir, Visual cryptography in Cryptology-Eurocryptâ€™94, Berlin, Germany:Springer-Verlag, pp. 1-12, 1995.
[23] C.-N. Yang and T.-S. Chen, Colored visual cryptography scheme based on additive color mixing, Pattern Recognit., vol. 41, no. 10, pp. 3114-3129, Oct. 2008.
[24] Y.-C. Hou, Z.-Y. Quan, C.-F. Tsai and A.-Y. Tseng, Block-based progressive visual secret sharing, Inf. Sci., vol. 233, pp. 290-304, Jun. 2013.
[25] H. Kuwakado and H. Tanaka, Size-reduced visual secret sharing scheme, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol. E87-A, pp. 1193-1197, 2004.
[26] C.-N. Yang and T.-S. Chen, New size-reduced visual secret sharing schemes with half reduction of shadow size, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol. E89-A, no. 2, pp. 620-625, 2006



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY