Iberian Journals

Iberian Journal of Applied Sciences and Innovation

2022 vol 2, Issue2

Analysis of Crypto Market Transaction Tracking

Ali Yousef[1] , Yahya Ahmad[2]

[1,2] **Neumont College of Computer Science, Salt Lake City, Utah, USA**

Abstract

Despite being completely unknown for more than a decade, cryptocurrencies are now a trillion dollar worldwide industry with more than 4,000 different currencies available. Additionally, the decentralized nature of digital currencies has elevated the sector to a level where privacy and safe transactions are taken for granted. Market analysis, however, indicates that there are numerous security flaws that could jeopardize the genuine anonymity of the bitcoin transaction network. In this post, we examine a few network security flaws that affect cryptocurrency systems.

Keywords: digital currency, tracking, transactions

1. Introduction

The paper by Biryukov et al. [1] examines vulnerabilities in cryptocurrency traffic that enable the identification of these features and the ability to link transactions to particular nodes in the network. Although this research shows that vulnerabilities can be exploited as expected, it also shows that the strategy utilized in this paper is increasingly valid in light of network applications used in the real world [2-4].

Biryukov [1] took a more detailed look at the flaws that integrating Tor and Bitcoin showed. Due to greater privacy concerns while employing the latter, this is typically done. This study found that this hybrid use creates weaknesses that can be exploited to make Tor useless and anonymize Bitcoin transactions. Although the ethics of this study can be questioned, the research's findings are particularly valid because the methodology used genuine Bitcoin systems, the Tor network, and the involvement of the systems' creators.

The paper by Apostolaki et al. [5] investigates the middleware routing and attack vulnerabilities in the cryptocurrency network. These attacks can be used to fully split and disconnect nodes in the Bitcoin network, according to research. The researchers demonstrate how a user's mining activities may be compromised and seriously harm the Bitcoin industry in this manner. While this strategy is similar to that in the first article, it takes a closer look at the practical uses of the vulnerability and shows how it has already been used in the Bitcoin network [6,7].

2. Research statement

The security flaws of cryptocurrencies are examined at the network level in all of the evaluated articles, but they are all examined from different angles. The first and second articles primarily discuss user-level flaws, while the third article focuses on other flaws [8]. These articles analyze network data to test the proposed vulnerabilities and determine whether it would be feasible for adversaries in the actual world to employ the examined attack vectors and the necessary resources [9].

The study by Biryukov et al. [1] examines Bitcoin network traffic. A hypothesized and investigated Bitcoin network vulnerability enables a user to bind traffic via network analysis on network nodes. To give a comparative perspective of the vulnerabilities of various cryptocurrencies, this analysis initially examines Bitcoin traffic before applying it to other privacy-focused cryptocurrencies.

The article by Biryukov et al. deals with a more focused vulnerability discovered in bitcoin communications as a result of combining the Tor browser with Bitcoin infrastructure. This pairing is thought to be a result of both the inclination to increase user privacy through the use of an anonymous browser, such as Tor, and the rising perception of privacy problems connected with Bitcoin traffic [10-12]. As a result of widespread flaws in the Tor network system traffic and Bitcoin, it has been suggested that this combination will lessen network anonymity. This article investigates the implications of this proposition. The discovered vulnerability enables the development of new attack vectors that can anonymously transmit user traffic using these platforms [13,14].

According to Apostolaki et al., the Bitcoin routing system is vulnerable to medium-sized attack vectors. This article examines security flaws in the architecture of Bitcoin network traffic that could be used to impair Bitcoin mining operations and economic activity. This article examines the same vulnerabilities we previously mentioned, which allow transactions to be connected with particular users and nodes; however, this issue is now being explored from a business perspective. It also evaluates the consequences of routing attacks and network fragmentation. In addition to the user-level ramifications covered in the essay by Biryukov et al., there may also be implications for Bitcoin itself.

3. Research methodology

Prior to the research by Biryukov et al., the flaws had not been thoroughly tested. The majority of other studies concentrated on using data mining techniques to analyze data taken from the blockchain [15-17]. This investigation reveals a mostly unprotected attack vector for all the cryptocurrencies under examination, even though its primary goal is to assess privacy-focused security mechanisms and vulnerabilities for cryptocurrencies.

This article expands on pertinent earlier research on anonymous attacks, which often involve just the initial network node to take part in a transaction. In spite of the requested transaction addresses, this study shows how to employ weight functions to link transactions to nodes. This study demonstrates that the network has flaws that can be used to identify transactions anonymously and with high accuracy across all cryptocurrencies examined in the study. Even adversaries with relatively limited resources are practically able to exploit the revealed vulnerability in the Bitcoin mainnet [18-20].

In their study, Biryukov et al. combined the use of the Tor anonymous browser and the Bitcoin network to identify novel attack avenues. The study looks at the potential for cookie misuse, which would enable assaults to track user transactions invisibly, as well as people's innate capacity to detect attacks when the two systems are merged. "Cookies" can save user fingerprints, making it possible to identify users when they connect to the Bitcoin network using Tor [21-25]. They can even help attackers locate and identify an IP address. This article also offers defenses that can be employed to deal with current privacy weaknesses.

Prior to the research presented in this paper, the topic of Bitcoin security on peer-to-peer systems has already been thoroughly investigated; nevertheless, by concentrating on the particular combination of Tor [26-28] and Bitcoin [29,30] traffic, two of the most well-known, this research offers a fresh perspective. Systems of their own kind also offer a patch to the system that fixes vulnerabilities that have been discovered [31-33], in addition to validating attack pathways in actual Internet contexts. Additionally, they provide particular countermeasures that can be applied to lower the risks [34,35]. In a study, Biryukov et al. investigated ways to attack Bitcoin networks. This article investigates assaults against digital currencies using network routing infrastructure and the Internet itself, despite the fact that several attack vectors have been established in the field of digital currency security. The research covered routing attacks and their effects on Chinese blockchain mining activities and their financial ramifications.

The analysis in the article, which shows both the likelihood of attacks and the fact that vulnerabilities are now being routinely exploited, challenges this idea. It is a typical issue with traffic redirection on the Bitcoin network. The provided research study offers compelling proof for the proposed attack vector, an estimate of the attack occurrence on real networks, and an assessment of the possible harm to Bitcoin and its users. These data come from empirical analysis and real network situations. This research presents both short-term and long-term countermeasures that can be utilized to enhance security and address issues presented by the research in addition to conclusively demonstrating flaws. By disclosing the methods and potential effects of this vulnerability on Bitcoin systems, researchers have significantly benefited the sector. The discovery of these vulnerabilities, especially considering the countermeasures introduced, has a substantial influence on the security of cryptocurrencies. It is also causing an increase in adversaries exploiting consumers in the market.

4. Experiments

The three examined papers examine security flaws in network traffic, so the study and analysis of the articles is done by evaluating the veracity of the researcher's proposed flaws in network traffic and Bitcoin transactions. Researchers can verify their assertions and determine what resources an adversary would need to use to launch an attack by performing attacks on their network traffic.

Humans are introduced to many middleware attacks in the article "Shutdown and Binding of Cryptocurrency Transactions Based on Network Analysis" that are used to listen for and gather information about network traffic passed through test nodes. In order to aggregate cryptocurrency transactions together and connect messages to suggested source nodes, this analysis is then utilized to create transaction weights and heat maps. Researchers try to link nodes with particular IP addresses using this aggregate data in an effort to significantly lessen

the secrecy surrounding cryptocurrency transactions. The enemy can further define node data by combining this data with additional information obtained from passive attacks, just like in a real-world attack, even though, as the researchers admit, this does not always produce conclusive results. The viability of the attack is evaluated using scenarios.

The "Bitcoin over Tor Idea Not Good" study article evaluates the claims made using the actual Bitcoin and Tor networks, unlike the prior paper that conducted an experiment on smaller experimental networks. In order to plan and carry out the suggested assaults, researchers' users were introduced into the network during this study on peer-to-peer network designs. The validity of the results is far higher than other publications conducted in tiny experimental contexts, which frequently fail to match the complexity of real-world network environments, because claims are examined in real-time using the Tor and Bitcoin networks. However, the utilization of actual user network data to test for vulnerabilities and exploits raises ethical questions about the research. These ethical concerns are lessened as a result of the necessary article updates because experiments were carried out in collaboration with the creators of Bitcoin and Tour and the "cookie address" attacks were immediately patched to fix the vulnerability.

Similar to the research carried out in [36,37], the researchers designed and investigated systems attacks that are carried out on smaller networks, and the findings are generalized by researchers to account for bigger network sizes that potential adversaries may confront in the real world. While this method has inherent faults that affect the validity of the researchers' conclusions, these problems are minimized by the thorough analysis done in the study, which pays close attention to how the exploitation will actually be used in the real world. In addition to these points, the researchers also showed how the flaws are currently being actively exploited on the actual Bitcoin network, where traffic has been successfully redirected and nodes have been compromised, thereby demonstrating the flaws in question.

5. Discussion

Although the three articles each make a unique technical contribution, they all add to the conversation around the privacy and security of cryptocurrencies. The authors of [38-40] examined flaws that were mainly ignored in earlier studies on the security of the digital currency. Both articles examine the issue of analyzing network traffic, the first from a user standpoint and the second from a corporate perspective. A topic that has been thoroughly studied before, the study paper "Bitcoin over Tor isn't a Good Idea" tackles the problem of digital currency security through peer-to-peer networks. The research however adopts a novel strategy by delving further into one of the most well-liked amalgamations of digital currencies and peer-to-peer networks.

The findings of the studies "Democratization and Possibility of Cryptocurrency Transactions Based on Network Analysis" and "Bitcoin Hijack: Directing Attacks on Cryptocurrency" point to serious threats to the security of the crypto network in hitherto unreviewed areas. Fundamental problems with the research that can cast doubt on the validity of the analysis's findings. First off, test settings might not accurately reflect how an assault might happen with a real attacker, as was briefly addressed in both articles. The environments employed for both publications were modest experimental environments that tended to neglect parts of the network security protocols used in actual cryptocurrency transactions, like publishing and

tethering, to closely imitate the actual situation the attacker faced. Separately, the test analysis results support the researchers' hypotheses regarding the flaws, however for the purposes of a straightforward analysis, other network security methods are disregarded [41]. When this is considered, the veracity of claims about security risk might be seriously contested. The probability-based approach yields much fewer results because real-world network architectures are much broader and more complicated than those evaluated in experimental situations. Due to these and other security mechanisms being ignored, the search results are a fairly poor approximation of the capability of actual attackers. However, as was already said, the extensive recovery in the use and variety of cryptocurrencies has given adversaries more and more industrial weaknesses to target, thus any flaws found in cryptocurrency systems can result in widespread exploitation. The researchers' statements about potential consequences are highly dubious, nevertheless, until the application of such a vulnerability in the actual world is established [42,43].

Along with the aforementioned, the research in [44,45] employs a technique similar to the first and actively investigates the drawbacks of utilizing such vulnerabilities in actual network environments. This study not only effectively supports their theory but also illustrates a potential method for combating abuse and the possibility of investigation supplying reciprocal actions. It also draws attention to the fact that the aforementioned vulnerabilities are already being used by adversaries in the Bitcoin network. Additionally, this article offers countermeasures that can be used in the short and long terms to address the vulnerabilities discovered through the study and analysis. The conclusions stated in [46,47] are substantially more credible as a result of a more thorough inspection and study of the proposed vulnerabilities and the identification of actual assaults on the Bitcoin network. Additionally, there are genuine vulnerabilities in the cryptocurrency network that not only need to be fixed right away but are actually costing Bitcoin and its miners money.

Using distinct beta environments, [48] carried out their investigation. While the authors themselves have evaluated and resolved the ethical issues raised by this vulnerability test, they have only done so in connection to the immediate effects of the experience on participants during study, taking no account of more general ethical standards. Tor's notoriety for enabling access to the dark web and the illegality of its use lead one to the conclusion that users who engage in illegal activity and commerce could dominate the combined use of Tor and Bitcoin. From this perspective, it can be inferred that finding and fixing vulnerabilities on these platforms is unethical, especially in light of the fact that law enforcement officials frequently use these attack vectors and vulnerabilities to look into and restrict illegal activities that rely on obscure platforms like the Tor browser [49]. Researchers, therefore, run the risk of undermining law enforcement attempts to stop unlawful and unethical activity on the Dark Web, like the sale of weapons, child pornography, and drug trafficking, by exposing these vulnerabilities and the solutions to fix them. However, the study methodology is thorough and rational, and real-world network settings used for research provide more valid results than the environment used for experiments, regardless of the ethical concerns of such research.

6. Conclusion

Over the past ten years, the cryptocurrency sector has grown rapidly, which has led to substantial advancements in systems and technology across the board. As a result of this

expansion, the security of these cryptocurrency systems has more flaws and weaknesses. The articles under examination examine some of the less well-known security flaws in cryptocurrency systems, with a special emphasis on Bitcoin and its network-wide flaws.

The analyzed articles give information about various cryptocurrency security flaws and potential attack routes. Although the articles mostly concentrate on Bitcoin, they also offer insights into other cryptocurrencies that prioritize privacy, like ZCash, Dash, and Monero. Given the current market domination of bitcoin, there is a lot of money at risk when evaluating the security of bitcoin systems, which has prompted the analysis of numerous attack avenues; nevertheless, some papers focus on some damage. They have less carefully considered flaws. They are most frequently seen at the network level in cryptocurrency systems. The articles "Bitcoin via Tor Is Not a Good Idea" and "Debugging and Correlation of Cryptocurrency Transactions Based on Network Analysis" discuss privacy concerns relating to Bitcoin network traffic vulnerabilities, especially at the user level. Bitcoin Hijacking: Routing attacks on cryptocurrencies continue to hunt for systemic flaws, however, these flaws are primarily commercial in nature and don't put much emphasis on user results.

Although the three articles focus on various facets of digital currency security, it is obvious that much work has to be done to protect cryptocurrencies, especially bitcoin, from possible attackers.

References

[1] Chaeikar SS, Jolfaei A, Mohammad N. AI-Enabled Cryptographic Key Management Model for Secure Communications in the Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems. 2022 Aug 29.

[2] Yazdanpanah S, Chaeikar SS, Jolfaei A. Monitoring the security of audio biomedical signals communications in wearable IoT healthcare. Digital Communications and Networks. 2022.

[3] Taherdoost, H., Sahibuddin, S., Namayandeh, M., Jalaliyoon, N., Kalantari, A. and Chaeikar, S.S., 2012. Smart card adoption model: Social and ethical perspectives. *Science*, *3*(4).

[4] Chaeikar SS, Jolfaei A, Mohammad N, Ostovari P. Security Principles and Challenges in Electronic Voting. In2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW) 2021 Oct 25 (pp. 38-45). IEEE.

[5] Fard, M. A. K., Bakar, K. A., Karamizadeh, S., & Foladizadeh, R. H. (2011, May). Improve TCP performance over mobile ad hoc network by retransmission timeout adjustment. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 437-441). IEEE.

[6] Shojae Chaeikar S, Tadayon M H, Jolfaei A, Alizadeh M. An intelligent cryptographic key management model for secure communications in distributed industrial intelligent systems. International Journal of Intelligent Systems.

[7] Karamizadeh, S., & Arabsorkhi, A. (2018). Skin Classification for Adult Image Recognition Based on Combination of Gaussian and Weight-KNN. International Journal of Information and Communication Technology Research, 10(2), 56-62.

[8] Yazdanpanah S, Shojae Chaeikar S, Zamani M, Kourdi R. Security features comparison of master key and IKM cryptographic key management for researchers and developers. In International Conference on Software Technology and Engineering, 3rd(ICSTE 2011) 2011. ASME Press.

[9] Karamizadeh, S., & Arabsorkhi, A. (2017). Enhancement of Illumination scheme for Adult Image Recognition. International Journal of Information and Communication Technology Research, 9(4), 50-56.

[10] Shojae Chaeikar S, Jafari M, Taherdoost H, Kar NS. Definitions and criteria of CIA security triangle in electronic voting system. International Journal of Advanced Computer Science and Information Technology. 2012 Oct;1(1):14-24.

[11] Dehzangi, A., Foladizadeh, R. H., Aflaki, M., & Karamizadeh, S. (2011). The application of fusion of heterogeneous meta classifiers to enhance protein fold prediction accuracy. In Intelligent Information and

Database Systems: Third International Conference, ACIIDS 2011, Daegu, Korea, April 20-22, 2011, Proceedings, Part I 3 (pp. 538-547). Springer Berlin Heidelberg.

[12] Shojae Chaeikar S, Razak SA, Honarbakhsh S, Zeidanloo HR, Zamani M, Jaryani F. Interpretative key management (IKM), a novel framework. In 2010 Second International Conference on Computer Research and Development, 2010 May 7 (pp. 265-269). IEEE.

[13] Azarnik, A. H. M. A. D., SHAYAN, J., ZADEH, S. K., & PASHANG, A. (2013). Lightweight authentication for user access to Wireless Sensor networks. In Proceedings of the 12th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications (EHAC'13), Cambridge, UK (pp. 35-39).

[14] Zamani M, Manaf AB, Abdullah SM, Shojae Chaeikar S. Correlation between PSNR and bit per sample rate in audio steganography. In11thInternational Conference on Signal Processing 2012 Apr 2 (pp. 163-8).

[15] Azarnik, A., Shayan, J., Alizadeh, M., & Karamizadeh, S. (2012). Associated risks of cloud computing for SMEs. Open International Journal of Informatics, 1(1), 37-45.

[16] Mazdak Z, Azizah BA, Shahidan MA, Shojae Chaeikar S. Mazdak technique for PSNR estimation in audio steganography. Applied Mechanics and Materials. 2012:1(229): 2798-2803.

[17] Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S., & Alizadeh, M. (2014). Identifying Benefits and risks associated with utilizing cloud computing. arXiv preprint arXiv:1401.5155.

[18] Chaeikar, Saman Shojae, Ahmadi, Ali, Karamizadeh, Sasan and Chaeikar, Nakisa Shoja. "SIKM – a smart cryptographic key management framework" *Open Computer Science*, vol. 12, no. 1, 2022, pp. 17-26. https://doi.org/10.1515/comp-2020-0167

[19] Alizadeh, M., Salleh, M., Zamani, M., Shayan, J., & Karamizadeh, S. (2012). Security and performance evaluation of lightweight cryptographic algorithms in RFID. Kos Island, Greece, 45-50.

[20] Zamani, M., Abdul Manaf, A.B., Zeidanloo, H.R. and Chaeikar, S.S., 2011. Genetic substitution-based audio steganography for high capacity applications. *International Journal of Internet Technology and Secured Transactions*, *3*(1), pp.97-110.

[21] Hooman, A., Marthandan, G., Yusoff, W. F. W., Omid, M., & Karamizadeh, S. (2016). Statistical and data mining methods in credit scoring. The Journal of Developing Areas, 50(5), 371-381.

[22] Sen J, editor. Cryptography and security in computing. BoD–Books on Demand; 2012 Mar 7.

[23] Alizadeh, M., Hassan, W. H., Zamani, M., Karamizadeh, S., & Ghazizadeh, E. (2013). Implementation and evaluation of lightweight encryption algorithms suitable for RFID. Journal of Next Generation Information Technology, 4(1), 65.

[24] Honarbakhsh S, Masrom M, Zamani M, Chaeikar SS, Honarbakhsh R. A Trust Based Clustering Model for Dynamic Monitoring in Ad hoc Network. InInternational Conference on Computer and Computational Intelligence (ICCCI 2010) 2010 Dec 25.

[25] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011). Enhancing congestion control to address link failure loss over mobile ad-hoc network. arXiv preprint arXiv:1110.2289.

[26] Shojae Chaeikar S, Ahmadi A. Ensemble SW image steganalysis: a low dimension method for LSBR detection. Signal Processing: Image Communication. 2019:70: 233-245.

[27] Dehzangi, A., & Karamizadeh, S. (2011). Solving protein fold prediction problem using fusion of heterogeneous classifiers. INFORMATION, An International Interdisciplinary Journal, 14(11), 3611-3622.

[28] Yazdanpanah S, Shojae Chaeikar S. IKM-based Security Usability Enhancement Model. IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS). 2012 Aug(4).

[29] Duan, W., Nasiri, R., & Karamizadeh, S. (2019, December). Smart city concepts and dimensions. In Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City (pp. 488-492).

[30] Alizadeh, M., Hassan, W. H., Behboodian, N., & Karamizadeh, S. (2013). A brief review of mobile cloud computing opportunities. Research Notes in Information Science, 12, 155-160.

[31] Shojae Chaeikar S, Manaf AA, Alarood AA, Zamani M. PFW: polygonal fuzzy weighted - an SVM kernel for the classification of overlapping data groups. Electronics. 2020: 9, 615.

[32] Shayan, J., Abdullah, S. M., & Karamizadeh, S. (2015, August). An overview of objectionable image detection. In 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET) (pp. 396-400). IEEE.

[33] Yazdanpanah S, Shojae Chaeikar S. Secure SMS Method Based on Social Networks. International Journal of Scientific Research in Science, Engineering and Technology. 2016: 2(6): 368-376.

[34] Shojae Chaeikar S, Moghaddam HS, Zeidanloo HR. Node Based Interpretative Key Management Framework. In Security and Management 2010 (pp. 204-210).
[35] Shojae Chaeikar S, Ahmadi A. SW: a blind LSBR image steganalysis technique. In the 10thInternational Conference on Computer Modeling and Simulation2018 Jan 8 (pp. 14-18). ACM.
[36] Arab F, Zamani M, Karamizadeh S, Khodadadi T, Alizadeh M, and Shojae Chaeikar S. Comparison of Data Hiding Techniques for Video Watermarking Applications. 2022 The 7th International Conference on Computer and Communication Systems 2022 April 22-25.
[37] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011, May). Packet loss differentiation of TCP over mobile ad hoc network using queue usage estimation. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 81-85). IEEE.
[38] Shojae Chaeikar S, Zamani M, Chukwuekezie CS, Alizadeh M. Electronic Voting Systems for European Union Countries. Journal of Next Generation Information Technology. 2013 Jul 1;4(5):16.
[39] Zeidanloo, H.R., Manaf, A.B.A., Ahmad, R.B., Zamani, M. and Chaeikar, S.S., 2010. A proposed framework for P2P Botnet detection. *International Journal of Engineering and Technology*, *2*(2), p.161.
[40] Karamizadeh, S., Abdullah, S. M., Manaf, A. A., Zamani, M., & Hooman, A. (2013). An overview of principal component analysis. Journal of Signal and Information Processing, 4(3B), 173.
[41] Chaeikar, S.S., Yazdanpanah, S. and Chaeikar, N.S., 2021. Secure SMS transmission based on social network messages. *International Journal of Internet Technology and Secured Transactions*, *11*(2), pp.176-192.
[42] Manaf AB, Zamani M, Ahmad RB, Jaryani F, Taherdoost H, Shojae Chaeikar S, Zeidanloo HR. Genetic Audio Steganography. International J. of Recent Trends in Engineering and Technology. 2010 May;3(2).
[43] Karamizadeh, S., Abdullah, S. M., Halimi, M., Shayan, J., & javad Rajabi, M. (2014, September). Advantage and drawback of support vector machine functionality. In 2014 international conference on computer, communications, and control technology (I4CT) (pp. 63-65). IEEE.
[44] T. Khodadadi, Y. Javadianasl, F. Rabiei, M. Alizadeh, M. Zamani and S. S. Chaeikar, "A Novel Graphical Password Authentication Scheme with Improved Usability," 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), 2021, pp. 01-04, doi: 10.1109/ISAECT53699.2021.9668599.
[45] Karamizadeh S, Shojae Chaeikar S, Jolfaei A. Adult Content Image Recognition by Boltzmann Machine Limited and Deep Learning. Evolutionary Intelligence, 2022.
[46] Shojae Chaeikar S, Manaf AB, Zamani M. Comparative analysis of Master-key and Interpretative Key Management (IKM) frameworks. In Cryptography and Security in Computing 2012. InTech.
[47] Alizadeh M, Hassan WH, Zamani M, Khodadadi T, Shojae Chaeikar S. A prospective study of mobile cloud computing. International Journal of Advancements in Computing Technology. 2013;5(11):198-210.
[48] Zamani M, Manaf AA, Ahmad R, Jaryani F, Taherdoost H, Shojae Chaeikar S, Zeidanloo HR. A novel approach for genetic audio watermarking. Journal of Information Assurance and Security. 2010;5:102-11.
[49] Shojae Chaeikar S, Zamani M, Manaf AB, Zeki AM. PSW statistical LSB image steganalysis. Multimedia Tools and Applications. 2018:77(1):805-835.