Cryptology For Christ: Steganography, Evangelism, & Closed Access Countries

Kaelyn Haynie and Chris Jaus, CISSP

Abstract

Digital steganography offers secure, covert channels for data transmission, presenting unique applications for Christian evangelism in restricted regions, without breaking laws related to cryptography and privacy. This research explores the versatility of file-appending methods in digital steganography, which bypass traditional limitations on data size and type. Utilizing a full copy of the Bible in text form and a sample image in .png form, we showcased the efficacy and security of this steganography method. Results demonstrate not only high levels of data integrity but also an incredibly easy to use methodology for implementation, making it an effective tool for discreetly disseminating religious texts. While our experiment employs a simple technique and procedure for the ease of the potential user, a Christian evangelist can substitute the methods showcased with more advanced steganography when the use case calls for it.

Introduction and Research Question

Introduction: Digital steganography is rooted in the ancient practice of hiding messages and has evolved dramatically with the progression of technological advancements. In the Christian worldview, modern technology's ethical application is rooted in the creation mandate, garnered from Genesis 1:28 which commands mankind to subdue the earth and have dominion over it. The Bible tells of examples where people used technology, including examples where God directly instructs time-period specific technological application. For example, in Exodus 36, two men were charged with the task of using their technological skills in both craftsmanship and metallurgy to create objects for the divine purpose of housing the unique presence of the God of the Israelites. Exodus 36:1 says, *"Bezalel and Oholiab and every craftsman in whom the Lord has put skill and intelligence to know how to do any work in the construction of the sanctuary shall work in accordance with all that the Lord has commanded."* If Christians today are craftsmen in whom the Lord has put skill and intelligence, then the technology available today can help to fulfill God's mandate to them in the Great Commission to spread the Gospel, especially where traditional methods of evangelism face constraints or persecution.

Research Question: Can Technology be used in the service of the Great Commission? Jesus said in Mathew 28:19-20 (NASB) "19 Go, therefore, and make disciples of all the nations, baptizing them in the name of the Father and the Son and the Holy Spirit, 20 teaching them to follow all that I commanded you; and behold, I am with you always, to the end of the age." One of the biggest challenges facing evangelists and new believers in closed countries is their access to copies of Scripture. A promising yet unexplored method for discreetly transmitting text is appending data to the end of a file, called Append Insertion Steganography. This method is compatible with a variety of file types, avoids causing errors, and eliminates many restrictions on the size and type of hidden data. Numerous file formats contain an end-of-file (EOF) marker, which most file-reading applications ignore, allowing for additional data to be placed after it without issue. We predict that even under progressive scrutiny, the cover provided by Append Insertion steganography will permit evangelists disseminate religious texts without detection.

Methods

Technical Method: Appending data to a file's end is a particularly versatile approach to digital steganography. This method is compatible with a variety of file types, avoids causing errors, and eliminates many restrictions on the size and type of hidden data. Numerous file formats contain an end-of-file (EOF) marker, which most file-reading applications ignore, allowing for additional data to be placed after it without issue. Traditional steganography techniques often impose limitations on the type and size of messages that can be concealed within cover or carrier files. The most suitable carrier files are those designed solely for sharing and viewing. These files should also include some form of stop marker—either at the file's end or within its structure—which signals to the default application when to stop reading the data stream. This ensures that the resulting steganographic file can be opened without any resulting corruption.

Experiment Method: Of the 10 images participants were provided with, 5 of them contained religious imagery or indications of the spiritual affiliations of the photos' subjects. Some of these were subtle, such as a cross hung on a shadowed background wall, while others blatantly featured people in liturgical attire. Disregarding the context of the images, five images were chosen at random and were steganographically appended with a compressed text file of the Bible and then used in the experiment.

Deception Plan Method: To simulate the scrutiny that evangelists' communication might receive on a foreign nations watch floor, we conducted an experiment with three variable levels of deception in accordance with the Liberty Institutional Review Board. Our participant group was the Cybersecurity club, which provided us with our necessary variance of experience levels. The second variable was time, as we limited inspection time for the provided images to 10 minutes for all participants. Lastly, we divided the individuals into three evenly-skilled groups of 10 individuals, giving each group different inspection instructions. Group A was given no warnings about their images, Group B was told that their items were under suspicion, and Group C was warned that their items might be employing cryptographic/stenographic subterfuge. This was to compare the success rate in varying levels of suspicion. Our hypothesis was that despite varying levels of suspicion the simple steganography would still be effective.

Figure 1. A literal demonstration of Bibles hidden in plain sight. Made with DALL-E by Haynie, K. and Jaus, C., 2024.

Figure 2. The command to required for Insertion Append steganography.

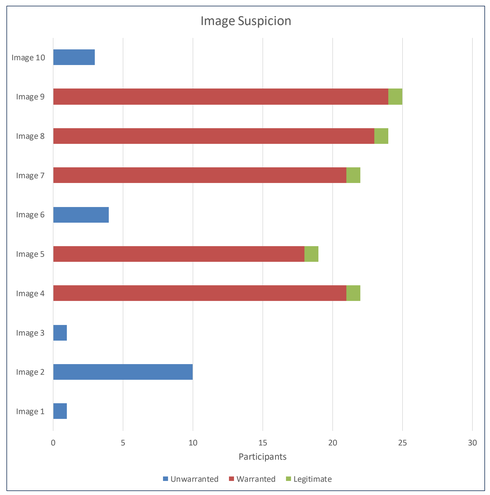

Figure 3. Suspicion of images as documented by participant notes. Unwarranted notes were taken on innocent images, warranted notes were included recognition of religious imagery on images employing steganography, and legitimate notes indicated suspicion of steganographic images warranted by technological evidence.

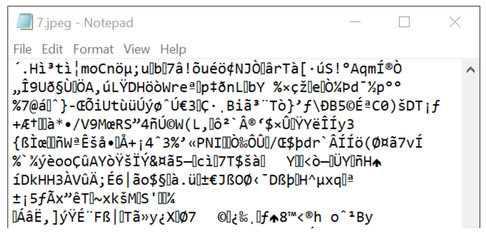

Figure 4. Data of a compressed Bible file at the end of an image file, viewed from a text editor.

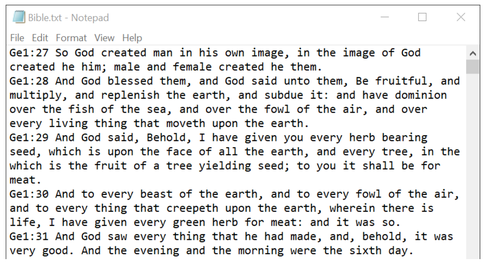

Figure 5. A Bible text file extracted with 7-zip from a steganography-appended image.

Results

Over the course of the experiment, the participants were shown a total of 150 Bibles hidden across the sample images. Two individuals (one from Group A, the other from Group C) experienced software or equipment failure prohibiting their participation. Despite the varying levels of experience, time-induced pressure, and differing amounts of suspicion represented by the three test groups**, not a single Bible was discovered**. Our simulation of a foreign watch floor demonstrates that append-insertion steganography is a plausible evangelism technique for missionaries in closed-access countries.

Conclusion

The first conclusion drawn is how the disparate skills can be brought together for God's glory. As we seek to go forward as ***Champions for Christ*** we hope to rally those around us to prayerfully seek the guidance of the Holy Spirit in all matters.

Our investigation reveals that appending data to the end of a file is an effective form of steganography that bypasses many limitations associated with traditional techniques, including file type and size constraints. The versatility of this method makes it particularly suited for the covert distribution of religious texts, such as the Bible. As we navigate the evolving landscape of digital communication, our study calls for further research into advanced methods that can continue to serve the Christian mission in a world where persecution of evangelists exist. This persecution is not new to Christianity, since Jesus himself recognized the inevitable risks of Christians sharing the Gospel to unbelievers. In Matthew 10:16, He says to his disciples, "Behold, I am sending you out as sheep in the midst of wolves, so be wise as serpents and innocent as doves." Steganography is a way in which Christians may use technology to be wise as serpents, and yet share the Gospel as perceptively harmless as doves.

Future Work

- Explore enhanced size reduction methods for steganographic content
- Extend this technique to other file types, specifically audio (.mp3) and video (.mp4) files
- Automate the append-insertion and recovery of a hidden file across multiple cover files
- Determine optimal public transmission channels for handling steganographic content

References

Akbari, A., & Gabdulhakov, R. (2019.) Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance and Society*, 17(1/2).

Donohue, J. W. (2001, December 1.) *Of Many Things*. America. https://go.openathens.net/redirector/liberty.edu?url=https://www.proquest.com/magazines/many-things/docview/209673367/se-2.

Evangelicals punished most by anti-evangelism law. (2019, July-August). *Christianity Today*, 63(6), 16. https://link.gale.com/apps/doc/A594553385/BIC?u=vic_liberty&sid=summon&xid=c3207795

Farrell, E. (1995, October 2). Christians imprisoned for proselytism. *Christianity Today*, 39, 108. https://go.openathens.net/redirector/liberty.edu?url=https://www.proquest.com/magazines/christians-imprisoned-proselytism/docview/211916341/se-2

Kumar, M. (2011.) *Steganography and Steganalysis of Joint Picture Expert Group (JPEG) Images* (Order No. 3496912). University of Florida. PROQUESTMS ProQuest Dissertations & Theses Global. https://go.openathens.net/redirector/liberty.edu?url=https://www.proquest.com/dissertations-theses/steganography-steganalysis-joint-picture-expert/docview/922399136/se-2.

Petitcolas, F. A. P., Anderson, R.J., & Kuhn, M.G. (1999.) Information Hiding: A Survey. *Proceedings of the IEEE*, 87(7), 1062–78. doi:10.1109/5.771065. Accessed September 2, 2023. https://www.petitcolas.net/fabien/publications/ieee99-infohiding.pdf.

Prasetyadi, G. C., Refianti, R., & Mutiara, A. B. (2018, February.) File Encryption and Hiding Application Based on AES and Append Insertion Steganography. *Telkomnika* 16(1), 361–7. https://go.openathens.net/redirector/liberty.edu?url=https://www.proquest.com/scholarly-journals/file-encryption-hiding-application-based-on-aes/docview/2031701378/se-2.

Rajesh Kumar Tiwari & G. Sahoo. (2011.) A Novel Methodology for Data Hiding in PDF Files. *Information Security Journal: A Global Perspective*, 20(1), 45–57. doi:10.1080/19393555.2010.544703.

Sarkissian, A. (2012.) Religion and Civic Engagement in Muslim Countries. *Journal for the Scientific Study of Religion*, 51(4), 607–22. http://www.jstor.org/stable/23353822.

Sharkey, H. J. (2004). Arabic Antimissionary Treatises: Muslim Responses to Christian Evangelism in the Modern Middle East. *International Bulletin of Missionary Research*, 28(3), 98-104.

Watheq, R. A., Almasalha, F., & Qutqut, M. H. (2018). A New Steganography Technique Using JPEG Images. *International Journal of Advanced Computer Science and Applications*, 9(11). https://go.openathens.net/redirector/liberty.edu?url=https://www.proquest.com/scholarly-journals/new-steganography-technique-using-jpeg-images/docview/2656433625/se-2.