Uma Plataforma para esteganografia em áudio

Guilherme S. Justino[1], Bruno N. Gomes[1], Daniel B. F. Conrado[1]

[1]Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais
Campus Sabará (IFMG)
CEP 34.590-390 – Sabará – MG – Brasil

{guidsjus}@gmail.com, {bruno.nonato, daniel.conrado}ifmg.edu.br

Abstract. *Since the Middle Ages, great civilizations have explored techniques for concealing messages, such as invisible inks, scalp pigmentation methods, among others. With the emergence of computer networks, many ill-intentioned individuals created various ways to attempt to steal information. On the other hand, there are those who strive to protect such information. From this issue arises the theme of this work: the use of audio steganography to conceal and hide information.The program applies the LSB (Least Significant Bit) technique to perform audio steganography with the distinctive feature of levels, in which the least significant bits are chosen based on the spacing of message insertion within the bytes. It also includes a function that traverses a byte array positioned in the level space to later retrieve the hidden message.The results indicate that smaller levels can hide larger messages but introduce audio distortion. Larger levels, on the other hand, can only conceal smaller messages but do not cause distortion in the audio.*

Resumo. *Desde a idade média, grandes civilizações exploraram técnicas de ocultação de mensagem, como, por exemplo, tintas invisíveis, técnica de pigmentação no couro cabeludo, entre outras. Com o surgimento de redes de computadores, muitas pessoas mal intencionadas criaram diversos meios para tentar roubar informações, assim, por outro lado, existem aqueles que tentam proteger essas informações. Com esse problema surgiu o tema desse trabalho: utilização de esteganografia em áudio para ocultar e esconder informações. O programa utiliza a técnica LSB (least Significant Bit) para fazer esteganografia em áudio com o diferencial dos níveis, onde o bit menos significativo são escolhidos através dos espaçamento de inserção da mensagem nos bytes e também possui a função que percorre um vetor de bytes posicionado no espaço dos níveis para descobrir a mensagem posteriormente escondida. Com os resultados, concluí-se que os níveis pequenos podem esconder uma mensagem maior, mas têm uma distorção no áudio. Os níveis maiores escondem uma mensagem pequena, mas não têm distorção no áudio.*

1. Introdução

A ocultação de informações vem sendo explorada ao longo dos séculos por meio de técnicas como tintas invisíveis, assinaturas digitais e canais escondidos. Há registros desde os tempos de Histieu, de Mileto e de Heródoto, no século V a.C., que relatou o caso de um mensageiro cuja cabeça foi raspada para que uma mensagem fosse tatuada em seu couro cabeludo; após o crescimento do cabelo, a mensagem ficava invisível. Até

meados do século XX, a ocultação de informações era utilizada predominantemente para fins militares (SCHÜTZ et al., 2009).

Nesse contexto, uma das áreas estudadas é a ocultação de mensagens por meio da esteganografia. O significado da palavra esteganografia vem do grego, onde a parte estegano significa ocultada, escondida, e grafia significa escrita. Logo, esteganografia significa escrita escondida (ROCHA et al., 2004). A esteganografia é uma técnica que consiste em ocultar uma mensagem no interior de outra, de forma que o remetente saiba a codificação ou sequência lógica da mensagem escondida. Diferentemente da criptografia, que torna perceptível a existência de uma mensagem, na esteganografia isso não é perceptível. No seu âmbito digital, a esteganografia pode a colocar informações e armazená-las em meios digitais, como fotos, músicas, textos e vídeos, onde técnicas de ocultação de mensagens são exploradas de diversas formas (ZANCHETT et al., 2021).

Com isso, o grande aumento de informações enviadas via Internet ou por redes privadas, surgiu uma necessidade de proteger os dados. Tornou-se primordial a garantia da confidencialidade das informações, pois essas são alvos de criminosos cibernéticos que desenvolvem diversas técnicas para roubar essas informações. Assim, a segurança de dados pode ficar comprometida, especialmente quando os dados não estão escondidos. Há um grande perigo de serem encontrados e roubados, e nem sempre a criptografia é suficiente, pois esta, sozinha, mostra que a mensagem está criptografada.

Portanto, diante da crescente necessidade de desenvolver técnicas de segurança da informação que não apenas protejam o conteúdo, mas também ocultem a existência de dados, surgiu a proposta deste trabalho o estudo e a aplicação de esteganografia como uma alternativa eficaz de proteção da informação. Logo, foi desenvolvido um software que utiliza a técnica LSB (*Least Significant Bit* – Bit Menos Significativo) para fazer a esteganografia em áudios no formato WAV. Como tal técnica adiciona distorções ao áudio, este software tem como diferencial o conceito de *nível*, que permite atenuar o nível de distorção. Quanto maior for o nível, menor será a distorção no áudio, mas menor será o tamanho máximo da mensagem que pode ser esteganografada no áudio. O programa também realiza o processo inverso, ou seja, faz a descoberta da mensagem que está no áudio.

2. Revisão bibliográfica

Diversas técnicas de esteganografia são exploradas na literatura, especialmente aplicadas a imagens e arquivos multimídia. No trabalho de (ZANCHETT et al., 2021), por exemplo, são analisadas comparativamente técnicas como **LSB** em Imagens em Escala de Cinza (*Least Significant Bit Grayscale* – **LSB** *Grayscale*), Sistema de Esteganografia Utilizando Bit 4 (*System of Steganography Using Bit 4* – **SSB-4**), Sistema de Esteganografia Utilizando Bit Pseudo-Aleatório (*System of Steganography Using Random Bit* – **SSB-N**), Transformada do Cosseno Discreto (*Discrete Cosine Transform* – ***DCT***), *Transformada Rápida de Fourier (Fast Fourier Transform* – **FFT**), entre outras. Todas essas técnicas foram avaliadas em imagens digitais e se mostraram eficazes na ocultação da informação de forma imperceptível ao olho humano.

(ZANCHETT et al., 2021) afirma que a técnica LSB é a abordagem mais comum na esteganografia, onde os *pixels* das imagens são utilizados para armazenamento de mensagens. Assim, dependendo da linguagem em que o algoritmo de esteganografia

é implementado, podem existir diferenças. Normalmente, o algoritmo recebe uma cópia da imagem original e faz uma manipulação de 32 bits dos pixels, onde o canal alfa, que representa o nível de opacidade, e os componentes RGB são manipulados, e a mensagem é transformada em código binário conforme a tabela ASCII. A mensagem em código ASCII é colocada bit a bit no vetor que possui alfa e RGB. Consequentemente, a imagem passa a conter uma mensagem, e as mudanças na imagem tornam-se imperceptíveis ao olho humano.

De acordo com (ZANCHETT et al., 2021) na técnica de LSB em escala de cinza, o uso das imagens nessa escala objetiva reduzir as distorções visuais ocasionadas pela técnica LSB. Assim, a mensagem, ao ser transformada em código ASCII e colocada nos bits menos significativos dos pixels (no alfa e no RGB), não provoca uma alteração tão agressiva na imagem.

A técnica de bit aleatório (SSB-N) em escala de cinza tem a mesma função da técnica de LSB em escala de cinza, mas, na hora de inserir os bits em código ASCII nos pixels em seu RGB, ela os adiciona aleatoriamente nos últimos 4 bits do RGB.

As técnicas de esteganografia por transformação de cosseno discreto são utilizadas para imagens que possuem partes redundantes. Essa técnica utiliza, para cada componente de cor, a transformação de cosseno discreto de blocos de 8x8 pixels em 64 coeficientes de uma transformação de cosseno direto e aplica equações de cosseno discreto em 2D. Após essa transformação, a mensagem é salva nos bits menos significativos. A técnica de esteganografia baseada em Transformada Rápida de Fourier é bem parecida com a técnica de Transformada do Cosseno Discreto, porém, utiliza um cálculo de Fourier em 2D. Finalmente, (ZANCHETT et al., 2021) faz uma comparação dessas técnicas e percebe que é impossível ao olho humano observar qualquer alteração em imagens processadas com quaisquer dessas técnicas de esteganografia.

(ZANCHETT et al., 2021)Os melhores resultados das técnicas de esteganografia em imagem foram obtidos pelas técnicas LSB na escala de cinza, SSB-4 em escala de cinza e modificação dos bits. Devido ao fato de ambas as técnicas modificarem principalmente os bits menos significativos do valor que representa a intensidade de cada píxel da imagem.

(ROCHA; COSTA; CHAVES, 2003) cria um software com o nome de Camaleão, voltado à segurança digital, utilizando a técnica LSB em Java. Assim, o software utiliza uma imagem de 32 bits, realiza a manipulação de cada pixel e de suas propriedades, e adiciona a mensagem, proveniente de outro arquivo, na imagem. O algoritmo possui uma chave simétrica que guarda, de forma aleatória, a distância entre cada bit que contém a mensagem. Essa chave possui um intervalo de $\{0, \ldots, m\}$, onde m denota o valor máximo. Sem o conhecimento da distância de cada bit, qualquer pessoa que tente descobrir a mensagem encontrará dificuldade e terá pouca chance de obter sucesso.

No processo de descoberta da mensagem, todos os bits menos significativos da imagem são extraídos e colocados em uma lista. Os bits são selecionados conforme a distância indicada em cada parte da chave simétrica. O resultado é uma imagem em que é impossível ao olho humano perceber qualquer diferença em relação à imagem original.

(CANTANHEDE, 2009) apresenta um programa que implementa técnicas de esteganografia usando o método LSB para ocultação de texto e imagem. Esse programa

possui duas funcionalidades: a criação do objeto esteganografado e a descoberta da mensagem em arquivos de imagem no formato PNG e áudio no formato WAV. As técnicas deste trabalho são aplicadas em arquivos PNG, pois outras extensões não satisfazem os requisitos da pesquisa. Após a inserção da mensagem, um arquivo estego é gerado. Neste trabalho, no momento da inserção de uma palavra em um arquivo de música ou imagem, são colocados dois marcadores: um de início e outro de fim. O resultado foi apresentado por meio de um histograma, que constatou a existência de alterações no arquivo nos locais onde a mensagem foi inserida, embora essas mudanças sejam indetectáveis ao ouvido e ao olho humano.

(AZEVEDO; FAVERI; NUNES, 2015) desenvolveu uma ferramenta web com interface simplificada para o envio de imagens. A primeira parte do processo consiste em carregar uma imagem com no mínimo três megabytes. Em seguida, a segunda etapa permite a inserção de uma mensagem na imagem, com limite de 225 caracteres. Após a seleção da mensagem e da imagem, inicia-se o processo de esteganografia. O algoritmo trabalha com a inserção de mensagens utilizando a técnica LSB. Na etapa de extração da mensagem, a frase é carregada, e ao final do processo, é possível realizar o download do arquivo. O resultado deste trabalho mostra que é impossível, a olho humano, detectar as alterações nas imagens em que as mensagens foram embutidas, atestando, mais uma vez, a eficácia da esteganografia feita com LSB.

(ESTEVAM, 2017) desenvolveu uma ferramenta que utiliza a técnica de esteganografia LSB em imagens, juntamente com o método de criptografia simétrica baseado no algoritmo simétrico, desenvolvido pela IBM na década de 70, com chave de 64 bits, dos quais 8 são de paridade. Na ferramenta, é possível inserir mensagens criptografadas em imagens. A outra parte da codificação tem a função de extrair as mensagens das imagens. Foi selecionado um texto com 239 linhas, que foi criptografado e inserido em uma imagem. Como resultado, é impossível, a olho humano, detectar qualquer alteração na imagem.

3. Metodologia

O software desenvolvido neste trabalho utiliza a técnica LSB para realizar esteganografia em arquivos WAV, com um diferencial: a introdução de níveis de esteganografia. Esses níveis representam o espaçamento entre os bytes do vetor de arquivo do áudio que recebem os bits da mensagem oculta. Logo, se o nível escolhido for 3, então, a cada três bytes, um bit da mensagem será adicionado ao final do byte. Isso se repete em cada nível, onde o espaçamento varia conforme o valor definido.

3.1. Funcionamento dos Níveis

- Nível 1: cada byte do áudio recebe 1 bit da mensagem no seu bit menos significativos.

- Nível 2: a cada dois bytes, um bit da mensagem é inserido no seu bit menos significativos.

- Nível N: a cada N bytes, um bit é embutido no seu bit menos significativos.

Assim, quanto maior o nível, menor a distorção no áudio, pois há menos alterações por segundo. No entanto, isso também reduz a capacidade de inserção da mensagem. A Figura 1 ilustra esse conceito de forma esquemática.

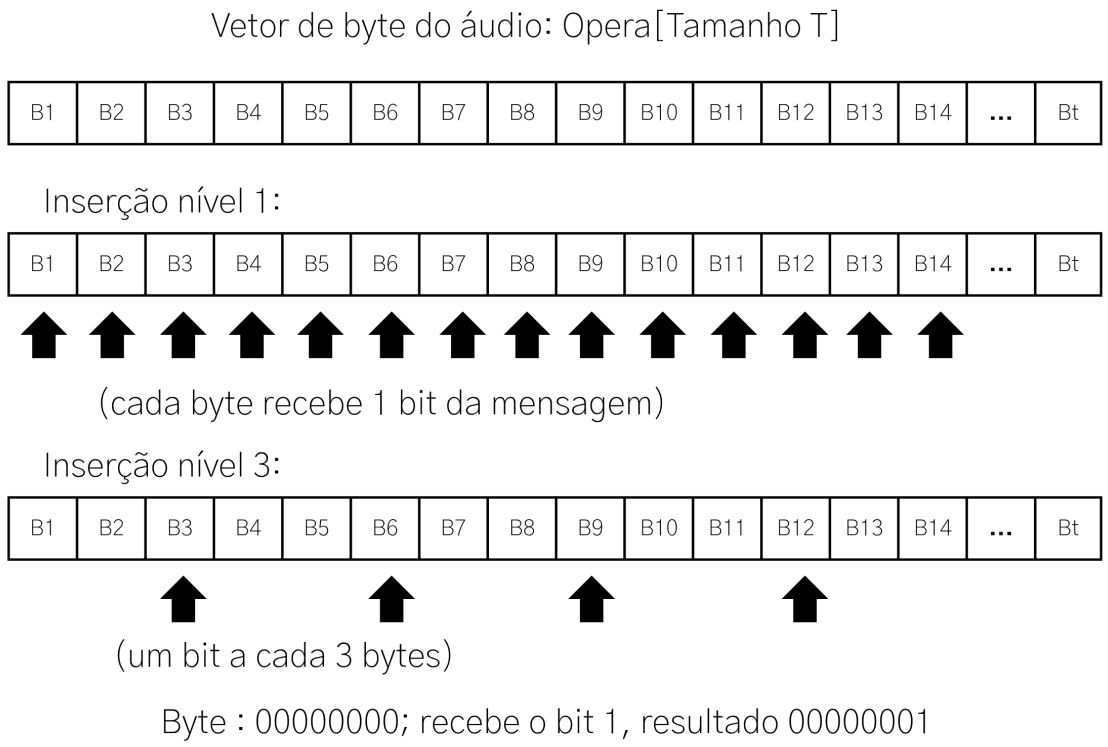

Figura 1. Funcionamento do nível

Para a extração da mensagem, o programa utiliza o nível definido e percorre o vetor de bytes, pegando o último bit menos significativo de cada posição do byte, conforme o espaçamento determinado. Esses bits são então reunidos para formar a mensagem, que é posteriormente salva em um arquivo de texto como mostra a 2.

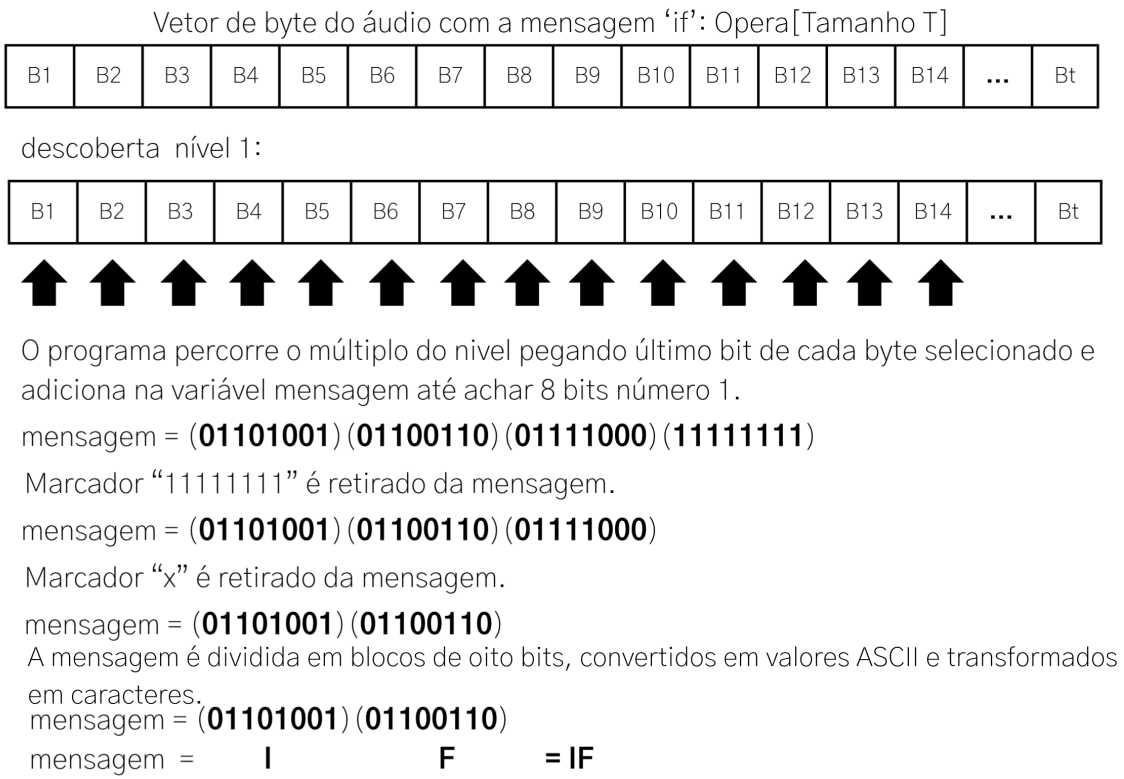

Figura 2. Descobrir Mensagem

O aumento do nível não altera a velocidade de inserção, mas diminui a quantidade de caracteres que podem ser inseridos no áudio. No entanto, como os áudios contêm uma quantidade enorme de bytes, essa limitação não afeta o resultado. Por exemplo, um áudio de 10 segundos no nível 50 comporta 8.427 caracteres, o que corresponde a cerca de duas páginas em tamanho A4 escritas em um recém criado documento em branco no Microsoft Word com a fonte Times New Roman 12 pontos tipográficos, espaçamento simples. Já o mesmo áudio no nível 100 na mesma fonte comporta 4.213 caracteres, o que é aproximadamente uma página. O resultado da alteração no áudio, em ambos os casos, é imperceptível ao ouvido humano.

Com isso, outros estudos podem ser baseados nas músicas, pois o algoritmo disponibiliza diversas variações da técnica LSB de esteganografia. Por exemplo, os primeiros níveis, de 1 a 5, podem utilizar músicas que possuam um instrumental com um vasto conjunto de sons, como uma orquestra filarmônica, black metal, músicas eletrônicas e seus diversos gêneros. No entanto, esses níveis não são recomendados para inserir mensagens longas, pois podem causar muitas distorções no som.

Por fim, como o programa possui diversos níveis de esteganografia, mais de 1000, podem surgir diversos estudos baseados nesses níveis. Por exemplo, quais músicas melhor se adéquam a determinado nível, qual é o melhor tamanho de mensagem para cada nível, qual mensagem se adequa melhor a uma música em um nível específico, e quais tipos de mensagens são mais compatíveis com determinados níveis.

3.2. Primeira tela

A primeira tela tem a função de mostrar ao usuário as duas funcionalidades do algoritmo realizar a esteganografia e descobrir a mensagem escondida na música. O botão número 1 abre a tela de esteganografia, enquanto o botão número 2 leva à tela de descoberta da mensagem oculta na música, como mostrado na figura 3.

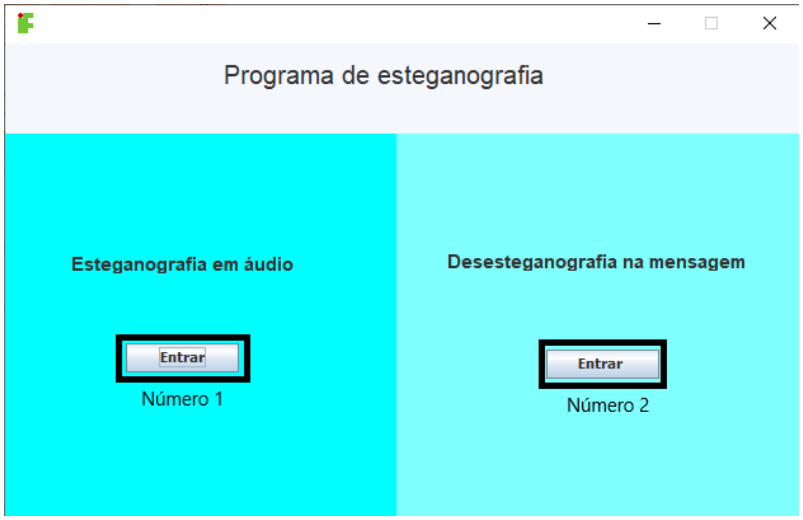

Figura 3. Primeira tela

3.3. Tela de esteganografia

A segunda tela do algoritmo possui o botão número 1, que abre uma janela para seleção de arquivos com extensão WAV. Após a seleção, a mensagem 'Caminho do arquivo' atrás do botão é substituída pelo caminho verdadeiro do arquivo selecionado. O botão número 2 abre uma janela para seleção do local onde o novo arquivo, contendo a mensagem esteganografada, será salvo, o usuário também pode alterar o nome desse arquivo. Após a seleção, a mensagem 'Caminho do arquivo' atrás do botão é atualizada para o caminho do arquivo criado. A área de digitação número 3 recebe o nível que será utilizado. O botão número 4 salva o nível selecionado, abrindo uma janela de confirmação, e o número atrás do botão é atualizado para o nível escolhido. A área de digitação número 5 recebe a mensagem que será esteganografada na música. O botão número 6 só pode ser acionado se todos os botões e etapas anteriores, exceto a seleção e a salvação do nível, forem executados; caso contrário, ele permanece inoperante. Após a conclusão de todos os passos anteriores, ao pressionar o botão número 6, inicia-se o processo de esteganografia, e o novo arquivo WAV é salvo no local escolhido pelo botão número 2. O botão número 7 tem a função de voltar para a tela anterior, conforme mostrado na figura 4.

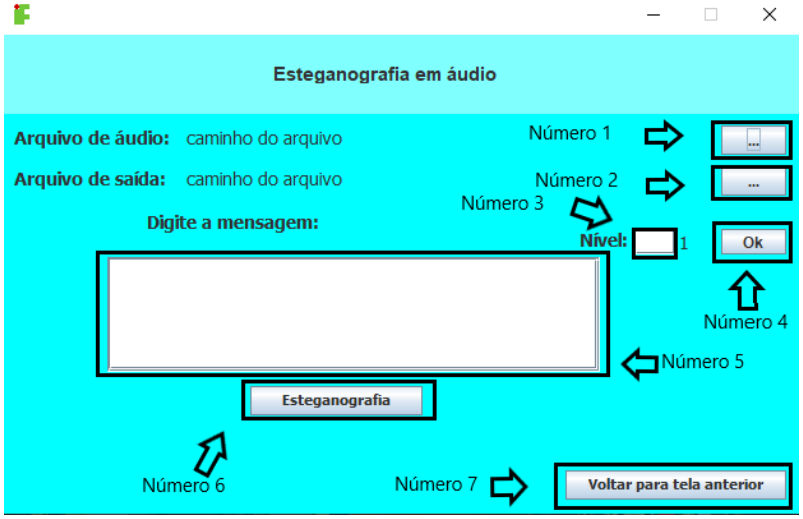

Figura 4. Segunda tela

3.4. Tela de Descobrir a Mensagem

Na terceira tela do algoritmo, o botão 1 possui a funcionalidade de abrir uma janela para seleção do arquivo WAV que contém a mensagem embutida. Ao selecionar o arquivo, a frase "Caminho do arquivo" localizada atrás desse botão é atualizada para exibir o caminho da música selecionada, que é então salvo. O botão 2 tem a função de escolher o local onde o arquivo de texto com a mensagem descoberta será salvo. Por padrão, o nome do arquivo é definido como "arquivo". Assim, a frase "Caminho do arquivo" atrás do botão 2 é atualizada para mostrar o caminho completo onde o arquivo será salvo. O campo de digitação 3 serve para inserir o número do nível desejado. O botão 4 inicia o processo de descoberta da mensagem, que só pode ser acionado após a seleção do arquivo e do local para salvar a mensagem, ou seja, após os botões anteriores terem sido usados e o arquivo salvo. O botão 5 salva o nível digitado no campo 3. Por fim, o botão 6 permite retornar à tela anterior. Como ilustrado na figura 5.

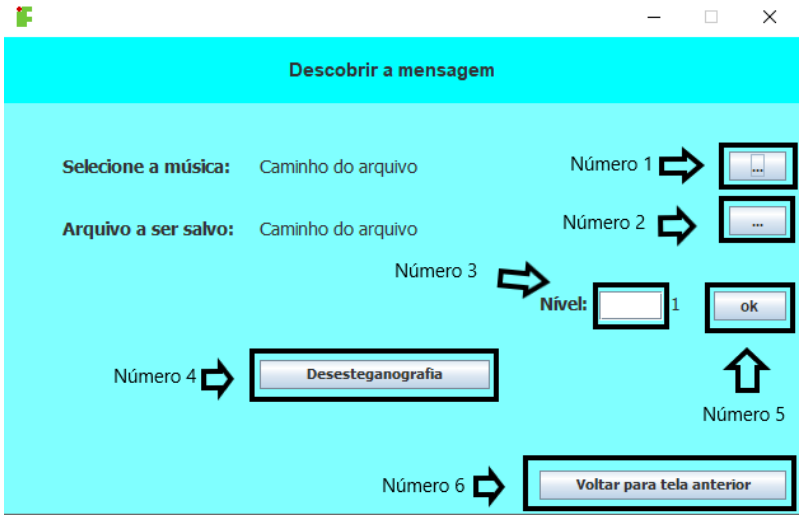

Figura 5. Terceira tela

3.5. Diagramas

Assim, com o diagrama de caso de uso apresentado na figura 6 onde o usuário tem acesso as duas principais funções do programa, sendo a tela de esteganografia e a tela de descobrir a mensagem. A primeira tem as principais funções de selecionar o arquivo de áudio, selecionar o caminho do arquivo final com a mensagem, digitar a mensagem, fazer a esteganografia, digitar o nível e a função de voltar à tela anterior. A segunda tem a função de selecionar a música que contem a mensagem, criar um arquivo de texto com a mensagem, digitar o nível, fazer a descoberta da mensagem e voltar à tela anterior.

O diagrama de sequência na figura 7 mostra a sequência de cada função do diagrama de caso de uso é utilizada e as possíveis respostas que o programa retorna para o usuário em sequência.

O diagrama de classe na figura 8, é possível compreender o funcionamento de cada tela do algoritmo, a interação do usuário com o sistema e a comunicação entre as classes, onde a classe TelaDaEsteganografia utiliza as classes Audio, MusicaEmbinario, Esteganografia, StringEmBinario para poder fazer a esteganografia e a classe TelaDeDescobrirMensagem utiliza a classe DescobrirMensagem para descobrir a mensagem. A classe PrimeiraTela utiliza as classes TelaDaEsteganografia TelaDeDescobriraMesagem para mostrar suas funções. Essas figuras estão apresentadas a seguir:

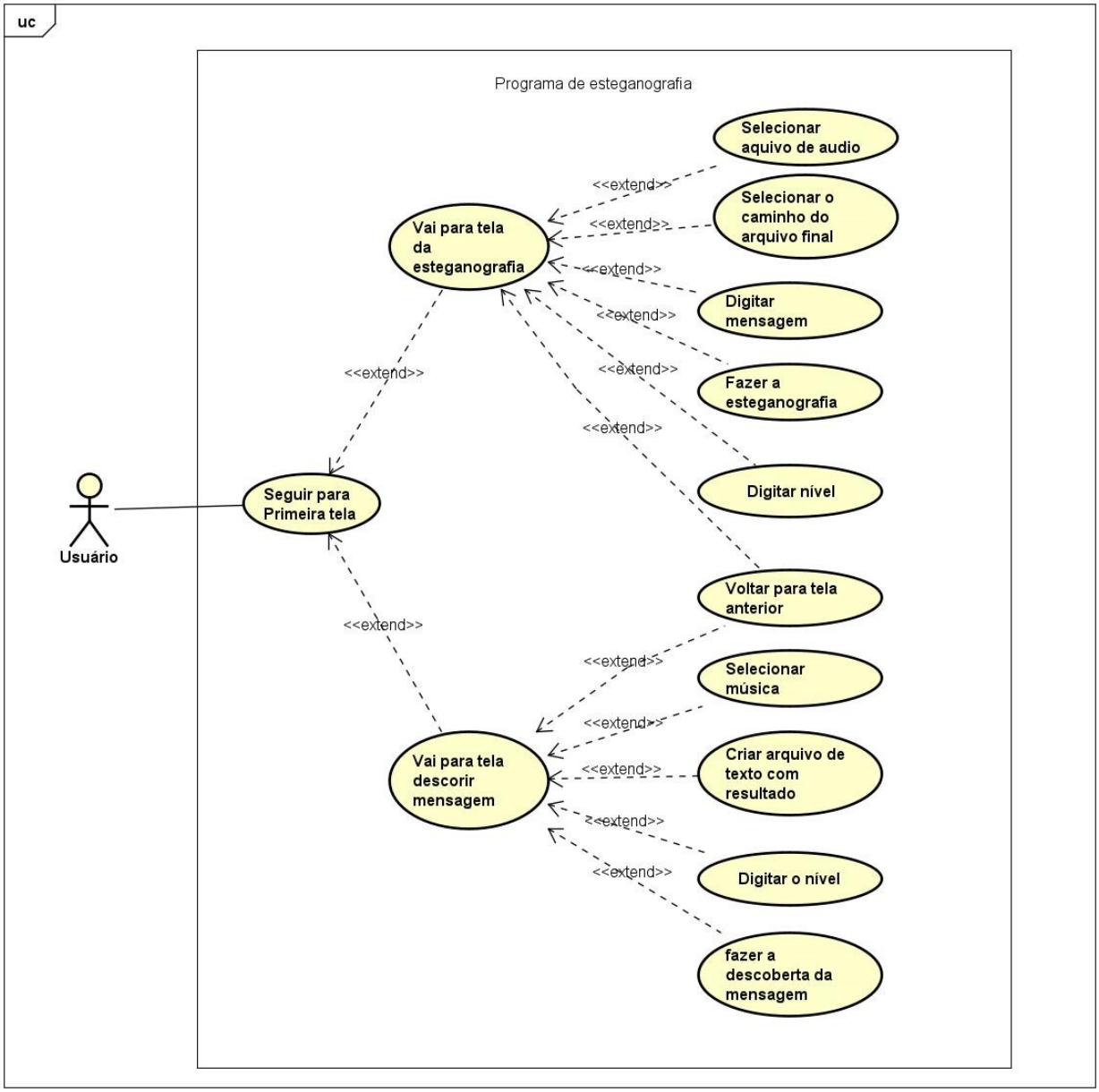

Figura 6. Diagrama de caso de uso

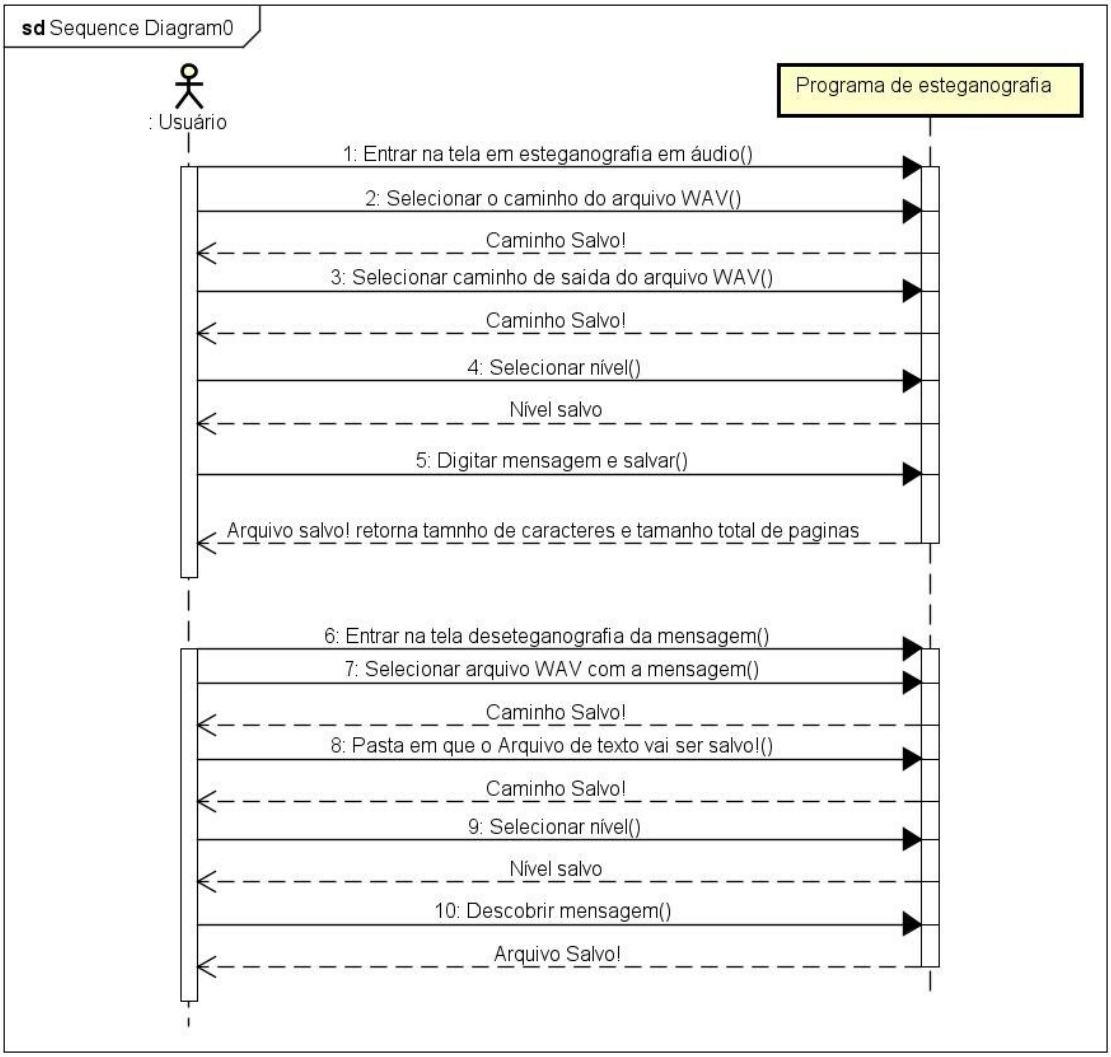

Figura 7. Diagrama de sequência

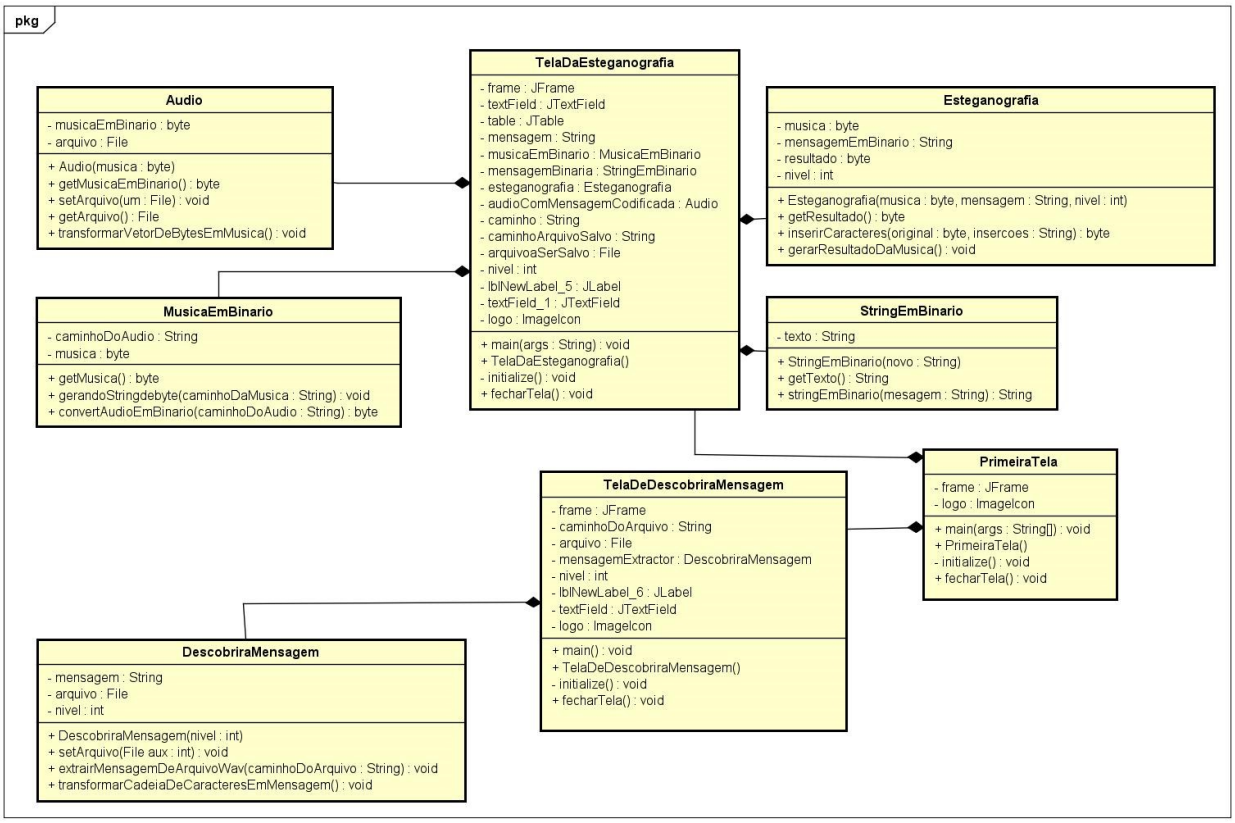

Figura 8. Diagrama de classe

3.6. Comunicação de objetos em cada classe de tela do algoritmo

A classe PrimeiraTela é responsável pela interface inicial do algoritmo, direcionando o usuário para uma das duas opções de funcionalidade disponíveis. Como suas funções utilizam pacotes nativos do Java, essa classe não faz uso de objetos de classes customizadas do sistema.

A classe TelaDaEsteganografia é responsável pela segunda tela do algoritmo e faz uso de diversos objetos de classes customizadas, tais como MusicaEmBinario, StringEmBinario, Esteganografia e Audio. Os respectivos objetos instanciados são: musicaEmBinario, stringEmBinario, esteganografia e audioComMensagemCodificada. Esses objetos atuam em conjunto para inserir uma mensagem nos bits menos significativos de uma música no formato WAV.

A classe TelaDeDescobrirMensagem é responsável pela terceira tela do programa e utiliza uma classe customizada chamada DescobrirMensagem, cuja função é extrair a mensagem oculta em um arquivo WAV. O objeto dessa classe é denominado mensagemExtractor.

4. Experimentos executados

Com o objetivo de validar o funcionamento do algoritmo desenvolvido, foram realizados diversos testes experimentais. Os experimentos buscaram analisar a capacidade do software em embutir mensagens em arquivos de áudio, a resistência da esteganografia a transformações no formato do arquivo, a percepção humana de alterações sonoras e os

limites de capacidade de inserção. A seguir, descrevem-se os principais testes realizados e os resultados obtidos.

4.1. Experimento 1 – Sobrescrição de Mensagem em Arquivo WAV

O experimento 1 tem o objetivo de verificar o comportamento do sistema ao tentar embutir uma nova mensagem de diferentes tamanhos em um áudio que já contém uma mensagem anterior. Durante o exprimento, uma mensagem foi inserida em um arquivo WAV. Em seguida, esse mesmo arquivo foi reutilizado no sistema para a inserção de uma nova mensagem.

Após o procedimento, viu-se que a mensagem previamente inserida foi completamente sobrescrita, confirmando que não há mecanismo de detecção ou preservação do conteúdo anterior. Ao aplicar o processo novamente, apenas a nova mensagem pôde ser recuperada.

4.2. Experimento 2 – Conversão de Formatos e Preservação da Mensagem

O experimento visa avaliar se a mensagem esteganografada é mantida após conversões entre formatos de áudio. Aqui, um arquivo WAV contendo uma mensagem foi convertido para o formato MP3 (com compressão), e depois reconvertido para WAV. Em seguida, foi utilizada a função de descoberta da mensagem.

Após o procedimento, a mensagem foi perdida durante a conversão. Isso confirma que o processo de compressão com perda, como o utilizado no formato MP3, destrói os bits menos significativos onde a informação estava armazenada.

4.3. Experimento 3 – Inserção de Mensagem com Capacidade Máxima

O experimento visa avaliar o comportamento do sistema ao inserir uma mensagem no limite da capacidade do áudio. Utilizou-se uma mensagem com o maior número possível de caracteres, de acordo com o nível e tamanho do áudio. O áudio resultante foi avaliado quanto à presença de distorções perceptíveis.

Como resultado observou-se que nos níveis mais baixos (ex: nível 1), havia alteração perceptível no som, especialmente em estilos musicais mais simples, como gravações de voz. Em contrapartida, em áudios mais complexos ou com instrumentos diversos, as alterações foram menos perceptíveis.

4.4. Experimento 4 - Cálculo da Capacidade Máxima de Inserção

O experimento visa determinar a fórmula e a aplicação prática para o cálculo do número máximo de caracteres que podem ser embutidos em um arquivo de áudio.termos da fórmula corresponde a CM e capacidade máxima, TB e tamanho do áudio em bytes, M e metadados e N e o nível. TB menos M calcula a quantidade de bytes, depois é dividido por 8 devido ao caractere possuir 8 bits, tira 2 caracteres devido à inserção automática no código e para finalizar divide pelo nível.

$CM = ((((TB - M)) \div (8))-2) \div N)$

Foram testados dois arquivos WAV com durações de 5 e 10 segundos, em diferentes níveis. Os resultados estão apresentados na Tabela 1.

Tabela 1. Quantidade de caracteres com em arquivos de áudio de diferentes durações e níveis

Duração do Áudio	Nível 1	Nível 25	Nível 50	Nível 100
5 segundos	110248	4409	2204	1102
10 segundos	421372	16854	8427	4213

4.5. Experimento 5 – Percepção Humana de Alterações Sonoras

O experimento visa avaliar a percepção de diferentes ouvintes quanto à presença de alterações no áudio esteganografado. três participantes na faixa de 18 a 30 anos e um músico na faixa de 31 a 50 anos. Esses escutaram diferentes estilos de áudio (rap, instrumental, gravações de WhatsApp e ópera) com mensagens embutidas nos níveis de 1 a 4, além de ouvirem o áudio original sem a mensagem, Os áudios foram escutados de forma aleatória. Cada participante classificou a percepção da alteração.

Os resultados, apresentados na Tabela 2, demonstram grande variação entre os participantes. Em geral, níveis baixos em áudios simples foram mais perceptíveis, enquanto músicas com instrumentação densa ou vozes sobrepostas ocultaram melhor as alterações. M representa modificado, NM significa não modificado e NI indica que a mensagem não pôde ser identificada. Assim, conclui-se que uma faixa de áudio com grande variedade de sons atende os primeiros níveis, enquanto uma faixa de áudio sem instrumental como um simples áudio de WhatsApp deve se atentar para usar níveis mais altos.

Tabela 2. Resultados da análise auditiva por participante

Áudio	Pessoa 1	Pessoa 2 (música)	Pessoa 3	Pessoa 4
Rap nível 1	NI	M	M	M
Rap nível 2	NI	NI	NM	NM
Rap nível 3	NI	NI	NM	NM
Rap nível 4	NI	NI	NM	NM
Instrumental nível 1	M	M	M	M
Instrumental nível 2	M	M	NM	NM
Instrumental nível 3	M	NM	NM	M
Instrumental nível 4	NM	NM	NM	NM
Gravação WhatsApp nível 1	M	M	M	M
Gravação WhatsApp nível 2	M	M	NM	NM
Gravação WhatsApp nível 3	M	NM	NM	NM
Gravação WhatsApp nível 4	NM	M	NM	NM
Opera nível 1	NI	M	M	NM
Opera nível 2	NI	M	NM	M
Opera nível 3	NI	M	NM	M
Opera nível 4	NI	NM	NM	M

5. Considerações Finais

Neste trabalho, foi desenvolvido um software de esteganografia em arquivos de áudio no formato WAV, utilizando a técnica dos bits menos significativos (**LSB – Least Significant Bit**) com a introdução de **níveis de espaçamento configuráveis**. A proposta visa não apenas ocultar a mensagem digital, mas também torná-la praticamente indetectável ao ouvido humano, contribuindo para a segurança da informação de forma discreta e eficiente.

A aplicação dos **níveis de esteganografia** mostrou-se eficaz para ajustar o equilíbrio entre **capacidade de inserção de dados** e **qualidade perceptiva do áudio resultante**. Níveis baixos permitem embutir grandes quantidades de dados, enquanto níveis altos minimizam distorções, tornando o método adequado para diferentes contextos. Os experimentos realizados comprovaram que, em níveis mais elevados, mesmo usuários com experiência musical não conseguiram identificar alterações sonoras. Além disso, testes demonstraram os limites da técnica quando confrontada com compressões de áudio, como a conversão para MP3.

Referências

AZEVEDO, E.; FAVERI, J. G.; NUNES, S. E. Esteganografia. *Revista de Ciências Exatas e Tecnologia*, v. 10, n. 10, 2015.

CANTANHEDE, H. S. Esteganografia emaudio e imagem utilizando a técnica lsb. 2009.

ESTEVAM, E. C. Segurança de dados com esteganografia e criptografia. *Revista Empreenda UniToledo Gestão, Tecnologia e Gastronomia*, v. 1, n. 1, 2017.

ROCHA, A. et al. Segurança e privacidade na internet por esteganografia em imagens. In: *Webmedia & LA-Web–Joint Conference 2004*. [S.l.: s.n.], 2004.

ROCHA, A. de R.; COSTA, H. A. X.; CHAVES, L. M. Camaleão: um software para segurança digital utilizando esteganografia. 2003.

SCHÜTZ, C. A. et al. Sistema de esteganografia em áudio digital que utiliza técnicas eficientes de inserção de dados. Pontifícia Universidade Católica do Rio Grande do Sul, 2009.

ZANCHETT, D. et al. Análise comparativa de métodos para esteganografia digital em imagens. *Anais do Computer on the Beach*, v. 12, p. 240–247, 2021.